1995

Health Information Privacy

Lawrence O. Gostin
Georgetown University Law Center, gostin@law.georgetown.edu

80 Cornell L. Rev. 451-528 (1995)

HEALTH INFORMATION PRIVACY

Lawrence O. Gostin†

Much of the academic and policy discourse on the health care system focuses on several fundamental goals: ensuring health coverage, equitable treatment, high quality services, and consumer choice at a reasonable cost for individuals, employers, and the federal and state governments.[1] The literature on health care systems characteristically defends the particular author's preferred plan for restructuring the market for health care services and/or financing of health insurance.[2] But achieving the goals listed above will require the development of a sound health information infrastructure,[3] irrespective of any changes to the organization and finance of the health care system. The ability of the health care system to function effectively depends in

---

† Associate Professor of Law, Georgetown University Law Center; Adjunct Professor, the Johns Hopkins School of Hygiene and Public Health; Co-Director, Georgetown-Johns Hopkins Program on Law and Public Health. J.D., Duke University, 1974; LL.D. (hon.), State University of New York, 1994. Although Professor Gostin chaired the Privacy Working Group of the President's Task Force on National Health Care Reform, the findings and conclusions in this Article do not necessarily reflect the views of the White House. Professor Gostin acknowledges the members of the Privacy Working Group: Joan Turek-Brezina, Madison Powers, Rene Kozloff, Ruth Faden, and Dennis Steinauer.

Professor Gostin wishes to thank Professors Anita L. Allen and Steven Goldberg of the Georgetown University Law Center; Rene Kozloff of Kunitz & Associates; Joan Turek-Brezina, Chair of the U.S. Department of Health and Human Services Task Force on the Privacy of Health Records; and John P. Fanning, Office of the Assistant Secretary for Health. He is also grateful for the research assistance of Barbara Looney and Marilyn Vadon. Finally, Professor Gostin acknowledges the support of the United States Centers for Disease Control and Prevention (particularly Verla Neslund in the Office of the General Counsel), the Council of State and Territorial Epidemiologists (particularly Willis Forrester), and the Task Force for Child Survival and Development of the Carter Presidential Center (particularly William C. Watson, Jr.) for enabling him to chair a national project on public health information privacy.

1 *See generally* Dan W. Brock & Norman Daniels, *Ethical Foundations of the Clinton Administration's Proposed Health Care System*, 271 JAMA 1189 (1994) (discussing the need for comprehensive insurance coverage, equal access to health care, high-quality medical services, individual choice in medical matters, and cost control); Lawrence O. Gostin, *Foreword: Health Care Reform in the United States—The Presidential Task Force*, 19 AM. J.L. & MED. 1, 2 (1993) (citing criticism of the current health system's failure to provide universal health care with equitable sharing of benefits and burdens).

2 *Compare* Eli Ginzberg, *Improving Health Care for the Poor: Lessons From the 1980s*, 271 JAMA 464 (1994) *and* Paul D. Wellstone & Ellen R. Shaffer, *The American Health Security Act—A Single-Payer Proposal*, 328 NEW ENG. J. MED. 1489 (1993) (authors with social welfare approaches) *with* Elizabeth McCaughey, *No Exit: What the Clinton Plan Will Do for You*, NEW REPUBLIC, Feb. 7, 1994, at 21 *and* Gail R. Wilensky, *Health Reform: What Will it Take to Pass?*, HEALTH AFF., Spring 1994, at 179 (authors who favor free market approaches).

3 For a definition of the term "health information infrastructure," see *infra* text accompanying note 24.

part on the accuracy, currency, completeness, and availability of health data.[4] All participants in the system (patients, health care providers, payers, researchers, and regulators) need high quality information for informed decisionmaking.

A health care system supported by data on almost any relevant subject, accessible to a diverse and significant number of users, is an integral part of the vision for health care reform.[5] Plans for the systematic collection, storage, use, and dissemination of a huge volume of uniform data sets in electronic form are already under way and have an aura of inevitability. This new health information infrastructure is the subject of reports recently published, or in press, by the Congressional Office of Technology Assessment,[6] the General Ac-

---

4 The term "health data" is broadly defined as all records that contain information that describes a person's prior, current, or future health status, including aetiology, diagnosis, prognosis, or treatment, or methods of reimbursement for health services. Lawrence O. Gostin et al., *Privacy and Security of Personal Information in a New Health Care System*, 270 JAMA 2487, 2488 (1993). Although these data are primarily held by members of the health care system (e.g., hospitals, health plans, and physician offices), the public health system (e.g., state or municipal health departments), and the health insurance system (public or private entities that provide reimbursement for health care services), such data also reside in an expansive array of record holders such as pharmacies, laboratories, researchers, and employers. *Id.* Even entities that have little or no relationship to the provision or payment of health care, like credit card companies, banks, and direct marketers, may hold or have access to health data. *Id.*

5 President Clinton's health care reform bill would have governed information systems and privacy and would bave established a national health information system: "The National Health Board shall develop and implement a health information system by which the Board shall collect, report, and regulate the collection and dissemination of the health care information . . . ." H.R. 3600, 103d Cong., 2d Sess. § 5101 (1994). Many other health care reform bills in Congress would have achieved the same result. *See, e.g.*, H.R. 1200, 103d Cong., 1st Sess. §§ 412, 486(A) (1993) (establishing the National Health Care Fraud Data-Base and the National Data System and Clearinghouse on Primary Care and Prevention Research, respectively); S. 1770, 103d Cong., 1st Sess. §§ 3301, 4121 (1993) (establishing health care data interchange system, and health care fraud and abuse data collection program, respectively). H.R. 1200 delineates the scope of such databases:

> The Director of NIH . . . shall establish a data system for the collection, storage, analysis, retrieval, and dissemination of information regarding primary care and prevention research that is conducted or supported by the national research institutes. Information from the data system shall be available through information systems available to health care professionals and providers, researchers, and members of the public.

H.R. 1200 § 486F, *supra*.

6 *See* CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY, OTA-CIT-296 (1986) [hereinafter OTA FEDERAL GOVERNMENT TECHNOLOGY]; CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION, OTA-TCT-576, 51-87 (1993) [hereinafter OTA PROTECTING PRIVACY]; CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT, THE QUALITY OF MEDICAL CARE: INFORMATION FOR CONSUMERS, OTA-H-386 (1988) [hereinafter OTA INFORMATION FOR CONSUMERS].

counting Office,[7] the National Academy of Sciences,[8] the Department of Health and Human Services,[9] the Physician Payment Review Commission,[10] and the Centers for Disease Control and Prevention.[11]

Contrary to the assertions of some privacy advocates, powerful reasons exist for the broad collection and use of health data. High quality data are needed to help consumers make informed choices among health plans and providers, to provide more effective clinical care, to assess the quality and cost effectiveness of health services, to monitor fraud and abuse, to track and evaluate access to health services and patterns of morbidity and mortality among underserved populations, and to research the determinants, prevention, and treatment of disease.[12]

Aggressive collection of a broad range of personal data, however, has a significant trade off in loss of privacy. American society places a high value on individual rights, autonomous decisionmaking, and the protection of the private sphere from governmental or other intrusion.[13] Americans currently believe that their privacy rights are not

---

7 *See* INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE, AUTOMATED MEDICAL RECORDS: LEADERSHIP NEEDED TO EXPEDITE STANDARDS DEVELOPMENT, GAO/IMTEC-93-17 (1993) [hereinafter LEADERSHIP NEEDED]; INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE, HEALTH CARE INFORMATION SYSTEMS: NATIONAL PRACTITIONER DATA BANK CONTINUES TO EXPERIENCE PROBLEMS, GAO/IMTEC-93-1 (1993); INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE, MEDICAL ADP SYSTEMS: AUTOMATED MEDICAL RECORDS HOLD PROMISE TO IMPROVE PATIENT CARE, GAO/IMTEC-91-5 (1991) [hereinafter MEDICAL ADP SYSTEMS].

8 *See* COMMITTEE ON REGIONAL HEALTH DATA NETWORKS, NATIONAL ACADEMY OF SCIENCES, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY (Molla S. Donaldson & Kathleen N. Lohr eds., 1994) [hereinafter HEALTH DATA IN THE INFORMATION AGE].

9 *See* TASK FORCE ON PRIVACY, U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY: CONFERENCE PROCEEDINGS (1993); FINAL REPORT OF THE TASK FORCE ON THE PRIVACY OF MEDICAL RECORDS, U.S. DEP'T OF HEALTH & HUMAN SERVS. (forthcoming, 1995); WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, U.S. DEP'T OF HEALTH & HUMAN SERVS., TOWARD A NATIONAL HEALTH INFORMATION INFRASTRUCTURE (1993).

10 *See* PHYSICIAN PAYMENT REVIEW COMM'N, ANNUAL REPORT TO CONGRESS 311-22 (1994) [hereinafter PPRC 1994]; PHYSICIAN PAYMENT REVIEW COMM'N, ANNUAL REPORT TO CONGRESS 27-54 (1993) [hereinafter PPRC 1993]; PHYSICIAN PAYMENT REVIEW COMM'N, ANNUAL REPORT TO CONGRESS 263-82 (1992) [hereinafter PPRC 1992].

11 The Centers for Disease Control and Prevention, the Council of State and Territorial Epidemiologists, and the Task Force for Child Survival and Development are overseeing a national study on the legal protection of public health and health care records with special emphasis on data held by government departments, including HIV and child immunization records. The GeorgetownJohns Hopkins Program on Law and Public Health is conducting the study with the author as principal investigator.

12 *See infra* notes 91-154 and accompanying text.

13 Concerns about privacy transcend the health care setting. *See Domestic and International Data Protection Issues, Hearings Before the House Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations*, 102d Cong., 1st Sess. (1991) (testimony of Alan F. Westin, Professor of Law and Government, Columbia Univer-

adequately protected.[14] In a 1993 Harris-Equifax poll specifically on health information privacy, eighty percent of the respondents believed that consumers had lost all control over how medical information about them is circulated and used.[15] Eighty-five percent of respondents said that protecting the confidentiality of medical records is an absolutely essential or very important part of national health care reform; they put this priority even ahead of providing universal coverage, reducing paperwork burdens, and providing better data for research into diseases and treatments.[16] Public fear and distrust of technology and bureaucracy are only likely to increase as collection, storage, and dissemination of information becomes more automated.[17] Health information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual. As the nation's health care system grows in size, scope, and integration, the susceptibility of that information to disclosure will also increase.

Thoughtful scholarship in the area of informational privacy[18] sometimes assumes that a significant level of privacy can coexist with

---

sity, and Academic Advisor to the Equity Survey, *How the American Public Views Consumer Privacy Issues in the Early 90's—And Why*); ALAN WESTIN ET AL., THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE (1990) *reprinted in id.* at 290; PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PRIVACY STUDY COMM'N].

14 Approximately 80% of those surveyed in public opinion polls consistently state that they are "very" (49%) or "somewhat" concerned (30%) about threats to their personal privacy in general. African Americans (86% concerned) and Hispanics (85% concerned) express higher levels of apprehension with 69% and 62% respectively, stating that they are "very" concerned about threats to personal privacy. ALAN F. WESTIN ET AL., HEALTH CARE INFORMATION PRIVACY: A SURVEY OF THE PUBLIC AND LEADERS 23 (1993) [hereinafter HEALTH INFORMATION PRIVACY SURVEY] (survey conducted for Equifax, Inc.).

15 *Id.* at 2; *see* David McNaughton, *Health Care Poll Finds Concerns About Privacy*, ATLANTA CONST., Oct. 29, 1993, at H3; C.B. Rodgers Jr., *It's Time for Serious Legislation to Protect Medical Privacy*, WASH. TIMES, Apr. 14, 1994, at A19 (chairman of Equifax, discussing the policy implications of the HEALTH INFORMATION PRIVACY SURVEY, *supra* note 14).

16 HEALTH INFORMATION PRIVACY SURVEY, *supra* note 14, at 10.

17 In the HEALTH INFORMATION PRIVACY SURVEY, *supra* note 14, at 66-67, 29% of the respondents stated that the fact that their health care providers use computers concerns them; strong majorities felt that computer use causes billing mistakes (75%), leads to inaccurate recordings of medical conditions (60%), and facilitates unauthorized disclosure of sensitive information (63%). *See also* Medical Records Inst., *The Challenge of the Next Two Decades*, TOWARD ELECTRONIC PATIENT REC., Dec. 1992, at 1; Jeff Goldberg, *Who's Reading Your Medical Records?*, LEAR'S, Nov. 1992, at 40.

18 Privacy, although a highly complex concept, can be defined as the right of individuals to limit access by others to some aspect of their persons. This Article focuses on informational privacy—the ability of an individual to deny others access to information regarding that individual. This Article is not concerned with decisional privacy—the freedom claimed by individuals to make intimate decisions about their bodily integrity without interference. *See generally* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 11, 31-34 (1987) (discussing definitions of privacy, including one that is specific to women's privacy concerns); Ruth Gavison, *Privacy and the Limits of Law*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 346 (Ferdinand D. Schoeman ed., 1984) (discuss-

the development of a modern health information infrastructure. Some commentators suggest that we can have it both ways: that adequate legal protection of informational privacy will eliminate the need to significantly limit the collection of health data. This Article demonstrates that there is no such easy resolution of the conflict between the need for information and the need for privacy. Because significant levels of privacy cannot realistically be achieved within the health information infrastructure currently envisaged by policymakers, we confront a hard choice: should we sharply limit the systematic collection of identifiable health care data in order to achieve reasonable levels of informational privacy? The result of that choice would be to reduce considerably the social good that would be achieved from the thoughtful use of health data. Alternatively, we may decide that the value of information collection is so important to the achievement of societal aspirations for health that the law ought not promise absolute or even significant levels of privacy at all, but rather should require that the data be used only for authorized and limited purposes. As I will show, the law at present neither adequately protects privacy nor ensures fair information practices. Moreover, the substantial variability in the law probably impedes the development of the kind of information systems envisaged; such systems require access to data in many jurisdictions, each of which has different legal standards.

Widely respected scholars such as Professor Alan F. Westin[19] and Professor Anita L. Allen[20] began the process of carefully scrutinizing the meaning and boundaries of the modern concept of privacy.[21] This Article builds on the work of these and other authors by developing a conceptual framework for a particular application of privacy—health information privacy.[22] The framework, like the earlier foundational work, requires a rigorous analysis of several central issues. First,

---

ing a neutral definition of privacy, privacy as a shared value, and privacy as a legal concept) [hereinafter PHILOSOPHICAL DIMENSIONS OF PRIVACY]; W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. PUB. AFF. 269 (1983) (exploring the definition and the moral and legal foundations of privacy); Judith J. Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra*, at 289 (exploring the lack of clarity in definitions of privacy and suggesting that privacy rights are derivative of other rights); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy [the Implicit Made Explicit]*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra*, at 272 (examining the extension of privacy rights to the realm of intangible property).

19 *See* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967) [hereinafter WESTIN, PRIVACY]; ALAN F. WESTIN, U.S. DEP'T OF COMMERCE, PUB. NO. 500-50, COMPUTERS, HEALTH RECORDS, AND CITIZEN RIGHTS (1976).

20 *See* ALLEN, *supra* note 18.

21 For other influential studies, see SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, PUB. NO. (OS) 73-94, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973); PRIVACY STUDY COMM'N, *supra* note 13.

22 Some thoughtful legal scholarship focused on this issue before the advent of modern automated health systems and the health care reform debate. *See, e.g.*, Wendy Parmet,

the health information infrastructure must be defined; its methods of collection, storage, use and transmission of information must be understood; and its public purposes must be evaluated. Second, the concept of informational privacy must be applied to health data in order to measure the probable diminution of privacy in a changing health care system, and the extent to which government can honestly keep a promise of privacy. Third, a careful examination of current constitutional, statutory, and common law must be undertaken to determine whether existing safeguards are adequate to protect health information privacy. Moreover, it is necessary to inquire whether current privacy safeguards are based upon antiquated concepts of how data are generated and used in a modern health system. Finally, ideas for balancing the public need for health information and individual claims to privacy must be generated. In an attempt to reconcile these equally compelling public and private claims, I will propose a federal preemptive statute based on fair information practices.

I
HEALTH INFORMATION INFRASTRUCTURE

The Institute of Medicine recently observed, "No one engaged in any part of health care delivery or planning today can fail to sense the immense changes on the horizon, even if the silhouettes of those changes, let alone the details, are in dispute."[23] The Institute was referring to the development of a national health information infrastructure, which I define as the basic, underlying framework of electronic information collection, storage, use, and transmission that supports all of the essential functions of the health care system.[24] These functions include clinical and prevention services, quality assurance, financial reimbursement, monitoring of fraud and abuse, research, and public health services.

Public Health Protection and the Privacy of Medical Records, 16 HARV. C.R.-C.L. L. REV. 265 (1981).

23 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 40. *See also* KAREN A. DUNCAN, HEALTH INFORMATION AND HEALTH REFORM: UNDERSTANDING THE NEED FOR A NATIONAL HEALTH INFORMATION SYSTEM 274-94 (1994) (explaining in nontechnical terms the role of information technology in alleviating the crisis in health care).

24 The U.S. Department of Health and Human Services lists the following components of a health information infrastructure: (i) "computer-based patient record (CPR) systems"—automated systems maintained by providers relating to specific patients, including clinical, administrative, and payment data; (ii) electronic networks—CPR systems that are "linked . . . through high-speed communication highways" using "standard definitions, codes, and formats that enable data to be universally recognized and processed"; (iii) "reference data bases—aggregate data from many patients"; and (iv) "computerized knowledge-based systems"—systems that "use decision logic and practice guidelines to help" health care providers with diagnoses and treatment, and evaluate outcomes of health interventions. WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, at 5.

A. The Automation of Health Data

Currently, most individual health records are kept manually in voluminous paper files. The General Accounting Office estimates that the 34 million annual hospital admissions and 1.2 billion physician visits could generate the equivalent of 10 billion pages of medical records.[25] These records are fragmented, poorly documented and duplicative; they are often not accurate, complete, timely, or accessible when needed for patient care.[26] "Information about a single episode of care could reside in the records of several different providers—history and symptoms in a physician record, laboratory results and surgical procedures in a hospital record, and rehabilitation in a home care agency record."[27] Further, there are no systematic operational models for the electronic storage of all aspects of health records.[28]

Despite the technical problems and the cost,[29] several governmental and private committees have proposed automation of health data,[30] and such automation is frequently discussed in the computer and health care literature.[31] The federal government specifically cites the need for access to health data as one of the driving forces behind

---

25 LEADERSHIP NEEDED, *supra* note 7, at 2 n.2. For earlier accounts of the sheer volume of paper records in the health care system, see INSTITUTE OF MEDICINE, THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE 12-14 (Richard S. Dick & Elaine B. Steen eds., 1991); PRIVACY PROTECTION STUDY COMM'N, *supra* note 13, at 277.

26 LEADERSHIP NEEDED, *supra* note 7, at 2.

27 WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, at v.

28 MEDICAL ADP SYSTEMS, *supra* note 7, at 21-22. The current inability to share medical information electronically stems largely from the lack of comprehensive standards for automated medical records, including standards for structure and content, messaging, and security. *See* Board of Directors of the American Medical Informatics Ass'n, *Position Paper: Standards for Medical Identifiers, Codes, and Messages Needed to Create an Efficient Computer-Stored Medical Record*, J. AM. MED. INFORMATICS ASS'N, Jan.-Feb. 1994, at 1 (proposing specific approaches to standardization in the areas of patient, provider, and site-of-care identifiers; computerized health care message exchange; medical record content and structure; and medical codes and terminologies).

29 *See* William M. Tierney et al., *Physician Inpatient Order Writing on Microcomputer Workstations: Effects on Resource Utilization*, 269 JAMA 379 (1993).

30 INSTITUTE OF MEDICINE, *supra* note 25, at 32-35; MEDICAL ADP SYSTEMS, *supra* note 7, at 5; WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, at v-x; WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, DEP'T OF HEALTH & HUMAN SERVS., OBSTACLES TO EDI IN THE CURRENT HEALTH CARE INFRASTRUCTURE at iii-v (1992).

31 *See, e.g.*, C. R. Gabriele & G. Murphy, *Computerized Medical Records*, 61 J. AM. MED. REC. ASS'N 26 (1990); Medical Records Institute, *The Process of Creating Electronic Patient Records*, TOWARD ELECTRONIC PATIENT REC. Oct. 1992, 1, 2. The mission of the Computer-Based Patient Record Institute, established in 1992 as a result of a report by the Institute of Medicine, is to "initiate and coordinate urgently needed activities to facilitate and promote the routine use of computer-based patient records throughout health care." COMPUTER-BASED PATIENT RECORD INSTIT., VISION STATEMENT (1992) (The Computer-Based Patient Record Institute (CPRI) is a consortium of provider groups, medical informatics experts, businesses, vendors, and insurers).

its initiative for a national information superhighway.[32] Three conceptual and technological innovations are likely to accelerate the pace of automation of health records: the development of a patient-based longitudinal health record, the assignment of a unique identifier to every American, and the eventual use of advanced technologies for health identification cards.

1. *Patient-Based Longitudinal Health Records*

The demand for accurate, complete, current, and accessible electronic data is emerging in an environment in which the existing automated systems are already undergoing significant change.[33] Although many health records have long existed in automated form, they have traditionally supported only specific functions, such as those of the laboratory, pharmacy, or finance department. A shift to patient-based longitudinal health records, now visualized as part of longer-term efforts toward building national health information networks, would fundamentally change the nature of existing record systems. Patient-based longitudinal health records are not merely automated versions of current records. They are patient-specific records in automated form containing all data relevant to the health of an individual (e.g., clinical, financial, and research-oriented information, including diagnostic images)[34] collected over a lifetime.[35] What is foreseen, then, is a single record for every person in the United States, continually expanded from prebirth to death and accessible to a wide range of individuals and institutions for a variety of purposes.

2. *Health Identification Cards and Unique Identifiers*

Under virtually all proposals for a national health care system, health identification cards would be issued to eligible persons, enti-

---

32 WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, at 8; *see* COMPUTER SYSTEMS POLICY PROJECT, PERSPECTIVES ON THE NATIONAL INFORMATION INFRASTRUCTURE: CSPP'S VISION AND RECOMMENDATIONS FOR ACTION 1 (1993) (calling for a public-private partnership to develop a national information infrastructure that would link institutions and resources throughout the country).

33 *See generally* MEDICAL RECORDS INSTIT., TOWARD AN ELECTRONIC PATIENT RECORD '94: TENTH INTERNATIONAL SYMPOSIUM ON THE CREATION OF ELECTRONIC HEALTH RECORDS AND SIXTH GLOBAL CONGRESS ON PATIENT CARDS (Peter Waegemann ed., 1994).

34 Medical imaging includes diagnostic images or pictures obtained from film scanners, computed radiography (CR), magnetic resonance (MR), computed tomography (CT), ultrasound, and nuclear medicine sources; the increasing digitization of data is rapidly expanding horizons for computerizing such images. INSTITUTE OF MEDICINE, *supra* note 25, at 65.

35 *See* Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform*, 23 HASTINGS CTR. REP., Nov.-Dec., 1993, at 13-14 ("Most envision a comprehensive electronic 'cradle to grave' medical file on every individual in the United States covered by health insurance.").

tling them to register and to receive certain health care services.[36] Even in the absence of national reform, health identification cards are likely to emerge at both the federal and state level. Health identification cards could be used in federal programs such as Medicare, Medicaid, and the Veterans Administration; in health care reform programs initiated by the states; and in health plans offered by large self-insured employers, health insurance companies, and health maintenance organizations that operate regionally or nationally.

Using health identification cards, eligible individuals would receive a unique identifier for the efficient operation of the health care system or health insurance plan. The unique identifier might be assigned at birth and stay fixed throughout the life span. It would be used for a variety of health, administrative, financial, statistical, and research purposes. It would provide access to care and to reimbursement for services rendered. The identifier would also point to the correct patient records, and establish longitudinal and geographic links among a patient's health care records in order to improve patient care, analyze patterns of health services, identify fraudulent activities, and provide a more detailed examination and evaluation of the health care system.[37]

Perhaps the most controversial decision regarding privacy and security in the use of health identification cards is whether to utilize the Social Security number (SSN) as the individual identifier. Almost all of the recent health care initiatives have proposed using the SSN as the unique personal identifier because it provides the most cost effective and timely method of identifying individuals and reliably collecting personal information.[38] However, the SSN at present is not a completely reliable identifier: it is not unique (there are multiple users of single numbers) and it is difficult to determine whether a random nine-digit number is a valid SSN. The process of verifying the identities of all holders and reissuing Social Security cards would cost between $1.5 to $2.5 billion.[39]

---

36 *See, e.g.*, Health Security Act, H.R. 1200, 103d Cong., 1st Sess. § 103(c) (1993) (eligible individuals are entitled to a health security card entitling them to a comprehensive benefits package).

37 *See* COMMITTEE OF EXPERTS ON DATA PROTECTION, THE INTRODUCTION AND USE OF PERSONAL IDENTIFICATION NUMBERS: THE DATA PROTECTION ISSUES 19-20 (1991).

38 *E.g.*, Health Care Cost Containment and Reform Act of 1993, H.R. 200, 103d Cong., 1st Sess. (1993); The Medieal and Health Insurance Reform Information Act of 1992, H.R. 5464, 102d Cong., 2d Sess. (1992). Other systems for assigning numbers were discussed in AMERICAN SOCIETY FOR TESTING AND MATERIALS, GUIDE FOR UNIQUE HEALTH CARE INENTIFIER MODEL (1993).

39 *Hearing on the Use of the Social Security Number as a National Identifier Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102d Cong., 1st Sess. 24-25 (1991) (statement by Gwendolyn S. King, Commissioner of Social Security).

According to those who support its wide-scale use in the new health care system, the SSN would create little additional risk to privacy. They argue that any unique identifier adopted for health care purposes would quickly end up in wide circulation. Certainly, a wide variety of authorized users would have access to the unique identifier, ranging from hospitals and health care providers to administrators, insurers, and regulators. Keeping unique identifiers truly private would be difficult. Further, Congress or possibly the executive branch could subsequently authorize use of the unique identifier to achieve other goals, such as identifying illegal immigrants.

To many civil libertarians, however, the SSN presents the gravest potential for privacy invasion that is possible with a unique health care identifier.[40] They are disturbed by the proliferation of the SSN for purposes unrelated to the administration of the Social Security system and the use of the number to uncover and link databases on many aspects of a person's life.[41] Since the SSN originated in 1936, it has been used extensively for a large variety of purposes that are not related to social security.[42] Although the Privacy Act of 1974 makes it unlawful for a government agency to deny a right, benefit or privilege because of a refusal to disclose a SSN, several federal departments do use these numbers, including the Internal Revenue Service, Department of Defense, Parent Locator Service, Food Stamp Program, and Selective Service system.[43] The SSN is also widely used in other government agencies and in the private sector, including debt collectors,

---

40 *See generally* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 15-16 (1989) (arguing there is a rational fear of the record linkages possible under a system using personal identification numbers); G.T. Marx, *The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures*, *in* THE SOCIAL FABRIC: DIMENSIONS AND ISSUES 135 (J.E. Short, Jr. ed., 1986) (arguing that advancing technology increases the totalitarian potential of democracy).

41 *See* SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *supra* note 21, at 121; ALAN E. WESTIN & MICHAEL A. BAKER, NATIONAL ACADEMY OF SCIENCE DATABANKS IN A FREE SOCIETY 399 (1972); Willis H. Ware, *The New Faces of Privacy*, 9 THE INFORMATION SOCIETY 195, 197-98 (1993).

42 *See* Greidinger v. Davis, 988 F.2d 1344, 1352 (4th Cir. 1993); OFFICE OF THE INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVS., THE EXTENT AND USE OF SOCIAL SECURITY NUMBERS at i-ii (1988); OTA PROTECTING PRIVACY, *supra* note 6, at 64-65; Ware, *supra* note 41, at 197-98.

43 Congress has given certain federal agencies statutory authority to use social security numbers. *See, e.g.*, 26 U.S.C. § 6109 (1988 & Supp. V 1993) (authorizing the use of social security numbers as identifiers for income tax purposes). In addition, the Privacy Act prohibition on the use of the Social Security number bas a grandfather clause. *See* Privacy Act of 1974, Pub. L. No. 93-579, § 7(a)(2)(B), 88 Stat. 1897. Thus, use of the social security number may have an explicit statutory foundation. The real privacy problem, therefore, is not necessarily legal, but a more basic policy problem (an instructive one). Congress can enact a law restricting the use of data on privacy grounds, but the pressures to use the data are considerable. A future Congress can authorize the use of the data for specific purposes, thus undermining the original privacy objective.

department stores, utilities, check validation services, supermarkets, cable television, credit card issuers, banks, major oil companies, mailing list companies, credit bureaus, insurance companies, the Medical Information Bureau, motor vehicle departments, law enforcement agencies, employers, schools, and universities.[44] The extensive use of the SSN in the public and private sectors leads to the concern that it has become a de facto national identifier.[45] One privacy advocate noted:

> Not only does the SSN make it easier for large institutions to compare their databases, it allows curious individuals (including private detectives, computer hackers or other strangers you might not want snooping into your private life) to 'hop' from database to database and draw out a profile of your buying habits and personal lifestyle.[46]

An alternative to the SSN that would better protect consumer privacy would be a number with no use other than for the health care system. Each person's health insurance number, then, would become just as private as his or her health record: disclosure of the number would be limited to those authorized to view the patient's health record; penalties would be established for unauthorized disclosure of the number; use of the number would be limited to approved health purposes; and the number could not be used to link health care databases with those found in other data systems.

3. *Electronic Card Technologies*

Future information systems incorporating unique identifiers may rely on advanced card technologies that are capable of storing substantial data on the card holder's health and finances.[47] Four types of plastic wallet-sized cards could be used for the collection, retention, use, and disclosure of portable files of personal information:[48] em-

---

44 In *Greidinger*, the Fourth Circuit Court of Appeals presented a detailed explanation of "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files" often unlocked by the SSN. 988 F.2d at 1353.

45 *See generally* JO ANNE C. BRUCE, PRIVACY AND CONFIDENTIALITY OF HEALTH CARE INFORMATION (2d ed. 1988); FLAHERTY, *supra* note 40, at 15-16, 406.

46 *Use of Social Security Number as a National Identifier, Hearings Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102d Cong., 1st Sess. 101, 106 (1991) (testimony of Evan Hendricks, publisher and editor, Privacy Times).

47 *See* TOM WRIGHT, HEALTH CARD TECHNOLOGY: A PRIVACY PERSPECTIVE (1992) 1-2 [hereinafter HEALTH CARD TECHNOLOGY]; OTA PROTECTING PRIVACY, *supra* note 6, at 55-64; Alpert, *supra* note 35, at 14.

48 HEALTH CARD TECHNOLOGY, *supra* note 47, at 3-4.

bossed,[49] magnetic strip,[50] integrated circuit,[51] and optical storage cards.[52] Integrated circuit cards that have the capacity not only to store information, but also to manipulate that information, are often called "smart cards."[53] Smart cards provide a medium for the storage of the equivalent of 800 printed pages. Since the mid-1980s, approximately 100 pilot projects using electronic card technologies have been initiated in health care systems internationally, including projects in Australia, Canada, France, Japan, Italy, Great Britain, and Sweden.[54] Although privacy advocates in the United States have expressed concern,[55] current health care proposals do not incorporate the use of electronic card technologies.[56]

Advocates of electronic card technology see it as a means of improving the accuracy, completeness, and accessibility of information. Smart cards hold the potential for improving the quality of health services (particularly emergency services), reducing paperwork, and containing costs associated with the processing of payment claims. Smart cards could also be used as part of an access control system to protect personal data. The memory of a smart card could be divided into several zones, each with different levels of access and security. Public zones could contain the card holder's identification while usage zones could contain emergency information, vaccination history, and medical history.[57] Confidential and secret zones could contain

---

49 The embossed card has raised letters containing only the information appearing on its surface. *Id.*

50 Magnetic strip cards add magnetic recording media to the back of an embossed card. While the stripes can hold up to 1200 bits of information or more, they are primarily used to access central databases. Access is obtained through use of the card in conjunction with a personal identification number (PIN). *Id.* at 3.

51 Integrated circuit cards utilize a microchip imbedded into an embossed card. Memory chip cards can be used only to store information. Smart cards can be programmed with sophisticated security and have the capacity to manipulate data without being connected to a central database. *Id.* at 3-4.

52 Optical storage cards use laser technology similar to that used for compact discs. Optical storage cards are being developed to hold up to 16 million bits of information and allow the storage of digitized images such as X-rays and ultrasound photographs. *Id.* at 4.

53 Smart cards are defined as "a credit card-sized device containing one or more integrated circuit chips, which perform the functions of a microprocessor, memory, and an input/output interface." OTA PROTECTING PRIVACY, *supra* note 6, at 55.

54 *See* HEALTH CARD TECHNOLOGY, *supra* note 47, at 7-10; INSTITUTE OF MEDICINE, *supra* note 25, at 78-79; OTA PROTECTING PRIVACY, *supra* note 6, at 59-62; Simon Davies, *Identity Cards: National Proposals Increase*, INT'L PRIVACY BULL., Apr.-June 1994, at 1.

55 *See, e.g.*, Mark A. Rothstein, *Taking the Patient's View of Health Care Reform*, J. AM. HEALTH POL'Y, Sept.-Oct. 1993, at 27; William M. Bulkeley, *Get Ready for Smart Cards in Health Care*, WALL ST. J., May 3, 1993, at B11; Williamson M. Evers, *'Smart Card' is Scary Proposal*, PLAIN DEALER, Nov. 6, 1993, at 7B.

56 WHITE HOUSE DOMESTIC POL'Y COUNCIL, THE PRESIDENT'S HEALTH SECURITY PLAN 124 (1993) ("The card itself contains a minimal amount of information.").

57 OTA PROTECTING PRIVACY, *supra* note 6, at 55-58 (citing MARTHA E. HAYKIN & ROBERT B.J. WARNAR, U.S. DEP'T OF COMMERCE, SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL 13-26 (1988)).

more sensitive information such as sexual or needle-sharing behaviors and psychiatric diagnoses.[58] Several technologies are available to restrict access to sensitive data, including personal identification, user verification, and cryptography.[59]

Sharp divisions exist as to whether smart cards would solve or exacerbate privacy problems in automated information systems. If smart cards were to replace central or linked databases, they could give consumers greater knowledge of information contained in their files, greater control over access, and tighter security. However, because smart cards would inevitably duplicate information contained in other systems, it is unlikely they would significantly increase informational privacy.[60] Smart cards would also have value to third parties for marketing, insurance, or media coverage of public figures, so they would be vulnerable to theft or fraudulent use.

B. Electronic Interchange of Health Data: The Development of Comprehensive Health Databases and Networks

The future health care information infrastructure will not merely contain automated records within each relevant institution. It will also electronically connect each of the vital components of the health care system, permitting the rapid exchange of health information and the processing of financial transactions.[61]

Health database organizations (HDOs) have already accelerated the process of collection, storage, and use of electronic data.[62] HDOs operate under the authority of government, private, or not-for-profit organizations. They have access to databases of health information and have as their chief mission the public release of data and of analyses performed on the data. HDOs serve specific geographic areas and

---

58 *Id.*

59 Cryptography is used to encode data in order to provide privacy, authenticate messages, and create digital signatures which protect against fraud. OTA PROTECTING PRIVACY, *supra* note 6, at 91. *See* CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT, DEFENDING SECRETS, SHARING DATA: NEW LOCKS AND KEYS FOR ELECTRONIC INFORMATION, OTA-CIT-310, 174-80 (1987) [hereinafter OTA DEFENDING SECRETS].

60 If information on the smart card were not duplicated or "backed up" in other systems, data essential to the patient's care might be lost, damaged, stolen, or forgotten when required for services.

61 WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, U.S. DEP'T OF HEALTH & HUMAN SERVS.: REPORT TO THE SECRETARY (1992). *See* WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, at 5.

62 Building on the proposal of the Institute of Medicine for health database organizations, the U.S. Centers for Disease Control and Prevention has recommended the establishment of "health data institutes" in every state charged with the design and production of "community health report cards." Edward L. Baker et al., *Health Reform and the Health of the Public: Forging Community Health Partnerships*, 272 JAMA 1276, 1279 (1994). "Using data generated by managed care providers, public health agencies, community hospitals, and other sources provided through new electronic networks, these institutes would provide extensive, up-to-date community health information." *Id.*

hold comprehensive health status data on all persons in a defined population.[63] HDOs acquire data from individual health records currently kept by physicians and hospitals. They also collect information from a wide variety of secondary sources: financial transactions from private insurance companies and government programs; public health surveillance and tracking systems; epidemiological, clinical, behavioral, and health services research; surveys conducted by government, academics, and private foundations; and numerous other data sources. The data collected include patient identified and patient identifiable data, as well as aggregate (nonidentifiable) data. They also include data on the performance of physicians and other health care providers.[64]

The development of population-wide health databases is not a distant concept, but a reality. At present, numerous health databases exist to support specific purposes.[65] These databases include information on medical cost reimbursement programs such as Medicaid or

63 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 54; *see* WHITE HOUSE DOMESTIC POL'Y COUNCIL, *supra* note 56 ("An electronic network of regional centers containing enrollment, financial, and utilization data is created.").

64 The Health Care Quality Improvement Act of 1986 (HCQIA), 42 U.S.C. §§ 11101-11152 (1988 & Supp. V 1993), established the National Practitioner Data Bank (NPDB), to support and encourage peer review and as a source of information for credentialing agencies. The NPDB, which is maintained by the Unisys Corporation under contract with the Department of Health and Human Services, serves as a central source of information concerning the practices of physicians. Barry R. Furrow, *Quality Control in Health Care: Developments in the Law of Medical Malpractice*, 21 J.L. MED. & ETHICS 173, 185 (1993). Information on medical malpractice actions, settlement claims, disciplinary actions, and decisions by health care facilities is contained in the database. 42 U.S.C. §§ 11131-11133 (1988 & Supp. V 1993).

65 *See, e.g.*, Rohert S. Boyd, *Medical Databanks' Expansion Spurs Privacy Fears*, ARIZ. REPUBLIC, Feb. 21, 1994, at A1 (discussing privacy implications of Arizona Medical Communications Network which links data systems in hospitals with private physicians and insurance carriers).

Medicare,[66] hospital discharges,[67] health status,[68] health policy research,[69] utilization and cost effectiveness,[70] specific diseases such as cancer,[71] and immunization registries.[72] Health databases are con-

---

66 HEALTH CARE FIN. ADMIN., U.S. DEP'T OF HEALTH & HUMAN SERVS., MEDICARE HOSPITAL MORTALITY INFORMATION, 1990 (1991); HEALTH CARE FIN. ADMIN., U.S. DEP'T OF HEALTH & HUMAN SERVS., MEDICARE HOSPITAL MORTALITY INFORMATION, 1986 (1987).

67 State statutes provide for collection of data for assessment of cost, utilization, quality-of-care, or a combination of the three. *See* ARIZ. REV. STAT. ANN. § 36-125.05 (1990); ARK. CODE ANN. § 20-8-110(a) (Michie 1987); CAL. HEALTH & SAFETY CODE § 443.31 (West 1991); COLO. REV. STAT. ANN. § 25-28-103 (West 1991); DEL. CODE ANN. tit. 16, §§ 2001-2004 (Supp. 1994); D.C. CODE ANN. § 32-325 (1993); FLA. STAT. ANN. § 408.05 (West 1994); GA. CODE ANN. § 31-7-281 (1982); HAW. REV. STAT. § 321-230 (1993); ILL. ANN. STAT. ch. 410, para. 52012 (Smith-Hurd 1993); IND. CODE ANN. § 16-21-6-6 (Burns 1993 & Supp. 1994); IOWA CODE ANN. § 145.3 (West 1991); KAN. STAT. ANN. § 65-6801 (1994); KY. REV. STAT. ANN. § 211.464 (Baldwin 1993); LA. CIV. CODE ANN. art. 40:2743 (West Supp. 1995); ME. REV. STAT. ANN. tit. 22, § 394 (West 1992); MD. CODE ANN., HEALTH-GEN. § 19-107 (1988); MASS. GEN. LAWS ANN. ch. 111, § 25A (West 1992 & Supp. 1994); MINN. STAT. § 62J.30 (1993); NEB. REV. STAT. § 81-676 (1994); NEV. REV. STAT. ANN. § 439A.082 (Michie 1991 & Supp. 1993); N.H. REV. STAT. ANN. § 126:1 (1990); N.J. STAT. ANN. § 26:2H-5.1 (West 1992); N.M. STAT. ANN. § 24-14a-3 (Michie 1978); N.Y. PUB. HEALTH LAW § 2803-b (McKinney 1991); N.C. GEN. STAT. § 131E-210 (1990); N.D. CENT. CODE § 23.01.1 (1991 & Supp. 1993); OHIO REV. CODE ANN. §§ 3732.11-.15 (Anderson 1994); 63 OKLA. STAT. tit. 63, §§ 5010-5015 (1994); OR. REV. STAT. § 442.120 (1989); 35 PA. CONS. STAT. §§ 449.1-19 (1991); R.I. GEN. LAWS § 23-17-10 (1989 & Supp. 1994); S.C. CODE ANN. § 44-6-170(c) (Law. Co-op. 1985 & Supp. 1994); S.D. CODIFIED LAWS ANN. 1-43-19 (1993); TENN. CODE ANN. § 68-1-108 (1992 & Supp. 1994); TEX. HEALTH & SAFETY CODE ANN. §§ 311.031-.038 (West 1991); UTAH CODE ANN. § 26-33a-104 (1993); VT. STAT. ANN. tit. 18, § 1952 (1993); VA. CODE ANN. § 9-166.1 (Michie 1993); WASH. REV. CODE ANN. § 70.170.100 (West 1991); W. VA. CODE § 16-1-10 (1990); WIS. STAT. ANN. § 153.05 (West 1989 & Supp. 1994); *see also* NATIONAL ASS'N OF HEALTH DATA ORG., THE STATE HEALTH DATA RESOURCE MANUAL: HOSPITAL DISCHARGE DATA SYSTEMS (1993); Douglas Sharrott, *Provider-Specific Quality-of-Care Data: A Proposal for Limited Mandatory Disclosure*, 58 BROOK. L. REV. 85, 104 (1992).

68 NATIONAL CENTER FOR HEALTH STATISTICS, U.S. DEP'T HEALTH & HUMAN SERVS., PUBLIC USE DATA TAPE: NATIONAL HEALTH INTERVIEW SURVEY, 1991 (1993).

69 AGENCY FOR HEALTH CARE POL'Y AND RESEARCH, AHCPR PURPOSE AND PROGRAMS (1990).

70 *See* JOSEPH P. NEWHOUSE, FREE FOR ALL? LESSONS FROM THE RAND HEALTH INSURANCE EXPERIMENT (1993).

71 The National Cancer Data Base, for example, was established jointly by the American College of Surgeons and the American Cancer Society in 1989. The database is the first large-scale national reporting system tracking trends in cancer treatments and their effects on cancer survival rates longitudinally. The database has two components: (1) a national tumor registry and (2) an assessment and surveillance mechanism consisting of a nationwide network of clinicians. The National Cancer Data Base Project, a joint project of the American College of Surgeons and the American Cancer Society, Chicago, IL, is discussed in Herman R. Menck, *A Preliminary Study of National Cancer Data Base Representatives: National Cancer Data Base Annual Review of Patient Care 1993*, CANCER NEWS, June 22, 1993, at 1.

72 Improved monitoring of disease and vaccination coverage is a central part of the Childhood Immunization Initiative launched by President Clinton. U.S. DEP'T OF HEALTH & HUMAN SERVS., THE CHILDHOOD IMMUNIZATION INITIATIVE (1994). The House and Senate Appropriations Committees included a small fiscal year 1994 funding allocation for the Department of Health and Human Services to establish a national immunization tracking system. Several congressional bills have proposed the development of a national registry system. *See, e.g.*, The Organ Transplant Program Reauthorization Act, H.R. 2659, 103d Cong., 2d Sess. § 6 (1994); Comprehensive Child Immunization Act, S. 732, 103 Cong., 1st

trolled by federal departments such as the Department of Defense[73] and Veterans Administration,[74] which are automating their health information systems across their medical treatment facilities worldwide; and the Public Health Service, which collects data on the health status of large populations.[75] The Department of Defense system includes a

---

Sess. (1993). Both the Centers for Disease Control and Prevention and the Robert Wood Johnson Foundation ("All Kids Count" Program) have funded municipal or statewide immunization registry systems that maintain core data on the vaccination history of children, including the name and several identifying characteristics of the child and parents. *See* Kay Johnson & Joel Breman, Immunization Registry and Reminder Systems: More Progress Needed to Increase U.S. Coverage Levels (Feb. 1994) (same) (on file with author). A few state and city health departments (e.g., Arkansas, Delaware, San Antonio, and Detroit) have developed automated immunization data systems. LARRY BLUMEN, CTRS. FOR DISEASE CONTROL, PROPOSAL FOR THE STATEWIDE IMMUNIZATION INFORMATION SYSTEM (1994). The New York City Health Department has also proposed legislation to establish an Immunization Registry. Board of Health, Dep't of Health, Notice of Intention to Adopt section 11.04 and Subsection (d) of Section 11.07 of the New York City Health Code (Nov. 9, 1993); *see also* Elizabeth R. Zell et al., *Low Vaccination Levels of U.S. Preschool and School-Age Children: Retrospective Assessments of Vaccination Coverage, 1991-1992*, 271 JAMA 833 (1994) (estimating percentages of preschool and school-age children by surveying school immunization records); *infra* note 117 (discussing immunization levels). Recently, the U.S. Department of Health and Human Services recommended a comprehensive immunization information system consisting of registries, computerized reminders, and recall. NATIONAL VACCINE ADVISORY COMM. ON VACCINATION REGISTRIES, U.S. DEP'T OF HEALTH & HUMAN SERVS., DEVELOPING A NATIONAL CHILDHOOD IMMUNIZATION INFORMATION SYSTEM: REGISTRIES, REMINDERS, AND RECALL (1994).

73 "The Composite Health Care System (CHCS) is a medical information system that the Department of Defense is developing for use in its more than 690 medical treatment facilities worldwide." INFORMATION MANAGEMENT & TECHNOLOGY DIV., GEN. ACCOUNTING OFFICE, CHCS DEPLOYMENT STRATEGY, GAO/IMTEC-91-47 at 1 (1991). CHCS is a state-of-the-art, integrated medical information system designed to improve the timeliness, availability, and quality of health care data. *Id.* at 2. "CHCS will replace manual and automated information systems now supporting Defense medical treatment facilities." *Id.* The GAO has been conducting a series of studies on integrated health information systems for the Department of Defense, the Veterans Administration, and nonfederal hospitals. *See* GENERAL ACCOUNTING OFFICE, ADP SYSTEMS: EXAMINATION OF NON-FEDERAL HOSPITAL INFORMATION SYSTEMS, GAO/IMTEC-87-21 at 3 (1987); *see also Technology/Private Sector One Step Ahead of Public Policy Debate in Health Care Reform*, PR Newswire, Apr. 1, 1994, *available in* LEXIS, Nexis Library, PRNEWS file (noting that integrated health information systems at U.S. military facilities around the world contribute to market demand for more efficient technologies).

74 The Veterans Health Administration (VHA) operates the Decentralized Hospital Computer Program (DHCP), the country's largest health information system. James M. Smith, *DHCP's a Tool for Health Care*, 10 GOV'T COMPUTER NEWS 109 (1991). The VHA's tool for delivering health care is in place at 167 hospitals, 229 outpatient clinics, 122 nursing homes, and 27 veterans homes. *Id.* at 109. These facilities support 1.1 million inpatients, 23.9 million outpatients and over 6 million records. *Id.* at 101; *see also* James M. Smith, *VA Acknowledges Software Problems*, 10 GOV'T COMPUTER NEWS 1 (1991) (describing management and technical problems with DHCP); *VA Asks for Vendors' Comments on Early Plans for HOST System*, 12 GOV'T COMPUTER NEWS 6 (1993) (describing the VA's Hybrid Open Systems Technology (HOST) program, developed in response to criticism of DHCP).

75 *See* NATIONAL CTR. FOR HEALTH STATISTICS, *supra* note 68; NATIONAL RESEARCH COUNCIL, PRIVATE LIVES AND PUBLIC POLICIES: CONFIDENTIALITY AND ACCESSIBILITY OF GOVERNMENT STATISTICS 15-43 (George T. Duncan et al. eds., 1993) (discussing how federal

comprehensive genetic database.[76] State agencies also maintain large databases, including integrated information systems as part of state health care reform.[77] Other health databases are established by hospital consortia, philanthropic foundations, or special authorities created under state law.[78] National, regional, and statewide databases are rapidly becoming repositories of a vast amount of information that could be of considerable interest for clinical, empirical, statistical, public health, epidemiological, educational, criminal justice, and commercial purposes.

One problematic source of information is previously stored tissue samples. Stored tissue samples may be regarded as inchoate data ba-

---

statistical agencies can preserve the confidentiality of their data and also meet the legitimate needs of users); Sandra Smith, *National Center for Health Statistics Data Line*, 108 PUB. HEALTH REP. 408, 409 (1993).

76 The DOD's Registry and Specimen Repository for Remains Identification was authorized by the Secretary of Defense on December 16, 1991, to serve as an improved method for the identification of soldiers' remains. Deputy Secretary of Defense Memorandum No. 47803 (Dec. 16, 1991) (not available for public release). Recognizing that modern warfare has the capacity to destroy human bodies beyond recognition by traditional fingerprint or dental analysis, the new system relies on DNA analysis to permit positive identification of remains, complementing these existing identification procedures. Memorandum from Enrique Mendez, Jr., M.D., the Assistant Secretary of Defense for Health Affairs, to the Secretaries of the Military Departments, Assistant Secretaries of Defense, General Counsel, and Assistants to the Secretary of Defense (Jan. 5, 1993) (regarding establishment of a repository of specimen samples to aid in remains identification using genetic deoxyribonucleic acid (DNA) analysis).

77 In April of 1992, Vermont enacted legislation to commence formal planning for a health care system that provides universal coverage to its citizens. Marilyn Moon & John Holahan, *Can States Take the Lead in Health Care Reform?*, 268 JAMA 1588, 1590-91 (1992). The method of providing care introduced and implemented by the state will emphasize integrated systems of care, with networks of physicians, hospitals, clinics, home health agencies, and mental health providers. Janice Somerville, *Vermont Reform on Schedule: Authority Unveils Two Reform Options*, 36 AM. MED. NEWS 2 (1993). To carry out this goal, the legislation creates a unified health care database. VT. STAT. ANN. tit. 18, § 9410 (Supp. 1994). This database, which is established and maintained by the Vermont Health Care Authority, is used to determine the capacity of existing resources, identify needs, evaluate effectiveness, compare costs of alternative approaches, and provide information to consumers and purchasers. *See* VT. STAT. ANN. tit. 18, § 9410(a)(1)-(5) (1993). For health care information systems established in other states, see NATIONAL ASS'N OF HEALTH DATA ORGS., THE STATE HEALTH DATA RESOURCE MANUAL: HOSPITAL DISCHARGE DATA SYSTEMS (1993); Edward L. Hannan et al., *Investigation of the Relationship Between Volume and Mortality for Surgical Procedures Performed in New York State Hospitals*, 262 JAMA 503, 504 (1989) (describing research based on a database maintained by the New York State Department of Health).

78 In 1980, nine Rochester hospitals joined with local Blue Cross, Medicare, and Medicaid offices to form a not-for-profit membership corporation, called the Rochester Area Hospitals Corporation, to cut the costs of health care in their community. *See* James A. Block et al., *A Community Hospital Payment Experiment Outperforms National Experiences: The Hospital Experimental Payment Program in Rochester, N.Y.*, 57 JAMA 193, 193-94 (1987). A health database was created to pool care information from all nine hospitals. *Id.* at 194-95. With the data received on inpatients, the corporation can provide both financial and clinical analyses to hospitals. *Id.* at 195; Ruthanne Sutor, *The Rochester Experiment*, FIN. WORLD, Jan. 10, 1989, at 18 (describing the success of the Rochester system).

ses because the technology exists to extract from them a vast amount of current and future health data.[79] The public health and research communities have shown increasing interest in using existing tissue samples for genetic testing and for creating new genetic databases.[80] In some cases genomic information is being extracted from large collections of tissue samples which were stored well before the advent of genetic testing; any consent that may have been obtained originally for tissue samples did not even envisage future genetic applications.

The most prominent example of an inchoate genetic database is the Guthrie spot program, whereby dried blood spots are taken from virtually all newborns throughout the United States.[81] The genetic composition of Guthrie spots remains stable for many years and, if frozen, can reveal genetic data indefinitely. A recent survey found that three-quarters of the states store their Guthrie cards, with thirteen storing them for over five years. Several states store these cards indefinitely, and a number of states express an intention to do so.[82] Only two states require parental consent for the blood spot.

Other tissue repositories have been created especially for genetic research. The federal government, for example, operates or funds a number of these DNA databases, such as the cancer tissue repository of the National Cancer Center of the National Institutes of Health. These government-operated repositories are obliged to comply with regulations designed, among other things, to ensure ethical review of human subject research.[83] Other repositories are purely private and remain unregulated. For example, the University of Utah has developed a human tissue repository for genetic research that is funded without federal dollars.

Perhaps the most ambitious public or private effort to create a database with both genetic and non-genetic applications is the National Health and Nutrition Examination Survey (NHANES) conducted by several federal agencies.[84] NHANES has collected comprehensive health status data in patient-identifiable form on some

---

79 Genetic research usually requires only DNA, which can be isolated from any nucleated cells. Tissue samples that can serve as DNA sources include not only solid tissues, but also blood, saliva, and any other nucleated cells. *See* Ellen W. Clayton, Informed Consent for Genetic Research on Stored Tissue Samples (July 7, 1994) (unpublished background paper for NIH/CDC Meeting on Informed Consent in Genetic Research, on file with the author).

80 *Id.*

81 For example, all states screen newborns for PKU and congenital hyperthyroidism, as well as other genetic defects.

82 Jean E. McEwen & Philip R. Reilly, *Stored Guthrie Cards as DNA "Banks"*, 55 AM. J. HUM. GENETICS 196, 196-97 (1994).

83 Protection of Human Subjects, 45 C.F.R. § 46 (1993).

84 DEPARTMENT OF HEALTH & HUMAN SERVS., NATIONAL HEALTH AND NUTRITION EXAMINATION SURVEY III (1994).

40,000 Americans in eighty-one counties in twenty-six states. This sample represents all population groups, with an overrepresentation of children, older persons, African Americans, and Mexican Americans. Each subject undergoes an extensive physical and dental examination. Some five hundred pieces of data are collected from each subject, ranging from socio-demographics, diet, bone density, and blood pressure, to risk status, drug use, and sexually transmitted diseases. Additionally, NHANES tests and stores biological samples for long-term follow-up and statistical research.

NHANES provides a classic illustration of a massive collection of highly personal and sensitive information by the federal government that has enduring societal importance. These data pose a significant risk of privacy invasion, but are critical to understanding health problems in the population.

C. A Health Information Infrastructure Under a National Health Care System

An organized strategy for the use of health information is an integral component of a national health care system.[85] The President's Task Force on National Health Care Reform,[86] together with most of the health care bills before Congress in 1994,[87] would have put in place a nationally coordinated system of health information. Any new proposals should include a method for collecting accurate and comprehensive data to inform consumer choice, monitor patient care, and assess system performance, as well as a method for sharing that data among system players and consumers.

It is important to emphasize, however, that even in the absence of health finance reform it is possible to create these methods of data collection and data sharing on a federal, regional, or state level. Legislative bodies could establish a Board or Commission or appoint an official with the responsibility to develop a health information strategy, set standards, and monitor the collection, use, and transmission

---

85 *The Informational Framework in the Health Security Act: Hearing on H.R. 3000 Before the Subcomm. on Census, Statistics and Postal Personnel of the House Comm. on Post Office and Civil Serv.*, 103d Cong., 2d Sess. (1994) (statement of Nan D. Hunter, Deputy General Counsel, U.S. Dept. of Health and Human Servs.). The several influential bodies that pressed the concept of a health information infrastructure all foresaw data systems as a necessary feature of reform. HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 1-2; PPRC 1993, *supra* note 10, at 27-54; PPRC 1992, *supra* note 10, at 263-82; WORKGROUP FOR ELEC. DATA INTERCHANGE, *supra* note 30, at 1-2.

86 WHITE HOUSE DOMESTIC POLICY COUNCIL, *supra* note 56, at 123-38.

87 *See* DIVISION OF DATA POLICY, DEP'T OF HEALTH & HUMAN SERVS., COMPARISON OF INFORMATION SYSTEMS AND PRIVACY PROVISIONS IN HEALTH CARE REFORM PROPOSALS (1994) (describing the bills); *see also* COMMITTEE ON NATL. STATISTICS, PRIVACY, CONFIDENTIALITY, AND STATISTICAL USES OF HEALTH CARE INFORMATION (1994).

of health data throughout the system.[88] A number of different types of data could be collected: eligibility and enrollment for the government health benefit or private insurance plans; patient encounters with health care providers; administrative and financial transactions; demographics; quality measurement, utilization, risk assessment, peer review, patient satisfaction, outcomes, and access; practice patterns for monitoring fraud and abuse; and health statistics and research results.[89] These data could be collected in a standardized format, both for administrative simplicity and to allow consistent measurements and comparisons within a national system.[90]

D. Assessing the Essential Purposes of a Health Information Infrastructure

It is not sufficient simply to present the health and financial objectives of a health information infrastructure. It is also necessary to measure the value of the efficient collection of information to the health and well-being of patients, as well as the cost savings to the health care system. Without a careful evaluation of the likely benefits of an organized health information strategy, it is impossible to assess whether the gains justify sacrificing a certain level of privacy.[91]

American society appears enamored with the power of information. Governments often claim a need to know certain information to achieve their purposes, whether it be national security, law enforce-

---

88 *See, e.g.*, Health Security Act of 1994, H.R. 3600, 103d Cong., 1st Sess. (1994) [hereinafter Health Security Act] (National Health Board is required to develop and implement a health information system (§ 5101) in conjunction with a National Privacy and Health Data Advisory Council (§ 5140)); Health Equity and Access Reform Today Act of 1993, S. 1770, 103d Cong., 1st Sess. (1993) [hereinafter Health Reform Today Act] (Health Care Data Panel, a federal panel chaired by the Secretary of Health and Human Services (HHS), develops the system, with regulations promulgated by the Office of Management and Budget; the Panel is advised by a National Health Informatics Commission); Affordable Health Care Now Act of 1993, H.R. 3080, 103d Cong., 1st Sess. (1993) (HHS Secretary adopts standards for data elements, uniform claim forms, and uniform electronic transmission of data; the Secretary consults with the Workgroup on Electronic Data Interchange and others and establishes an advisory commission); American Health Security Act of 1993, H.R. 1200, 103d Cong., 1st Sess. (1993) (American Health Security Standards Board comprised of the HHS Secretary and others); Managed Competition Act of 1993, H.R. 3222, 103 Cong., 1st Sess. (1993) (Health Care Standards Commission appointed by the President; the Benefit, Evaluations, and Data Standards Board, a nonprofit organization, advises the Commission); Health Care Information Modernization and Security Act of 1993, H.R. 3137, 103d Cong., 1st Sess. (1993) (Information system similar to Health Reform Today Act, *supra*); Medical and Health Insurance Information Reform Act of 1992, S. 2878, 102d Cong., 2d Sess. (1992) (HHS Secretary oversees state development of Comparative Value Information Programs for health care purchasing).

89 *See, e.g.*, Health Security Act, *supra* note 88, § 5101(e).

90 *See, e.g.*, Health Security Act, *supra* note 88, § 5102(b).

91 *See* Allan M. Brandt et al., *Routine Hospital Testing for HIV: Health Policy Considerations*, *in* AIDS AND THE HEALTH CARE SYSTEM 125 (Lawrence O. Gostin ed., 1990) (arguing for this approach).

ment, or public health;[92] health care providers often claim a need to know the full medical and behavioral history of patients, not only for clinical decisionmaking, but also for their own occupational safety;[93] and patients claim a right to know information about the benefits and risks of treatments and the qualifications and other characteristics of doctors in order to make informed decisions.[94] It is not surprising, therefore, to find that many advocates of a health information infrastructure simply assume that collection of ever increasing health information, in ever more efficient ways, is inherently a social good.[95] This assumption is not self-evident, however; it requires testing.

What exactly are the goals of a health information infrastructure and how could these goals be attained?[96] Overall, the goals are: (1) to guarantee the integrity of health data so that information is accurate, complete, current, and trustworthy, since the integrity of information is critical to quality patient care, assessment of services, research, and public health; (2) to ensure the availability of health data so that persons who need the information for legitimate health purposes have ready access to the data, since without readily available clinical information, providers cannot make informed decisions regarding diagnoses and treatment; and (3) to allow the administrative simplification of financial and other transactions, since burdensome and duplicative processing of transactions can significantly drive up the costs of providing health care.

Advocates of a health information infrastructure forecast a number of benefits, including the ability to enhance consumer

---

92 *See* Sarah McCabe, *National Security and Freedom of Information*, *in* CIVIL LIBERTIES IN CONFLICT 185, 185 (Larry Gostin ed., 1988) ("The acquisition, analysis, and prudent disposition of knowledge sometimes is and always should be the prime objective of every individual and of every state. . . . In [the government's] restricted sense of 'information,' however, it is clearly seen as a powerful instrument of control over destructive forces within and without state boundaries.").

93 For example, many clinicians claim the right to know if their patients are infected with the human immunodeficiency virus; in certain circumstances, such as following a needle stick accident, several state statutes grant them a right to know. *See* Larry Gostin, *Hospitals, Health Care Professionals, and AIDS: The "Right to Know" the Health Status of Professionals and Patients*, 48 MD. L. REV. 12 (1989); Larry O. Gostin, *Public Health Strategies for Confronting AIDS: Legislative and Regulatory Policy in the United States*, 261 JAMA 1621 (1989) (listing state statutes); *see also* David M. Bell, *HIV Infection in Health Care Workers: Occupational Risk and Prevention*, *in* AIDS AND THE HEALTH CARE SYSTEM 115 (Lawrence O. Gostin ed., 1990).

94 *See* Larry Gostin, *The HIV-Infected Health Care Professional: Public Policy, Discrimination, and Patient Safety*, 18 LAW, MED. & HEALTH CARE 303 (1990).

95 *See generally* U.S. DEP'T OF HEALTH AND HUMAN SERVS., HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY (1993) (proceedings of a conference sponsored by the U.S. Department of Health and Human Services, Washington, D.C., Feb. 11-12, 1993).

96 *See* INSTITUTE OF MEDICINE, *supra* note 25 (describing the advantages of computer-based patient records (CPRs) and proposing a plan for systemwide development of CPRs); HEALTH DATA IN THE INFORMATION AGE, *supra* note 8.

choice, improve the quality of health services, assess system performance, improve administrative efficiency, facilitate research, and safeguard public health.[97]

1. *Enhancing Consumer Choice*

Proponents of managed competition, a variation of which formed the core of President Clinton's health care plan,[98] have long regarded high quality information as an essential element of an efficient health care market.[99] Of course, informing and protecting consumers "ought to be a valued end in itself, not just a means to a working health care marketplace."[100] Under almost any health care system, consumers have to make a number of important decisions. Consumers have to choose a health plan and a primary care provider. Moreover, they must make numerous decisions about health services such as which specialist or hospital best meets their needs. At present, consumers can rarely base their decisions about health services upon clear and relevant information.

Most importantly, under classic managed competition theory, consumers in the present system cannot realistically make informed choices about health care or insurance plans. These plans have a numbing variety of benefits, services, and prices that make it virtually impossible for the average consumer to make intelligent comparisons. For example, if a dozen health plans exist in a given market, with each plan publishing a detailed prospectus of covered conditions, exclusions, capitations, and preexisting conditions in a nonuniform format, even the most studious consumers will have difficulty making an informed choice. By requiring all health plans to provide the same core benefits package, proponents of managed competition expect that consumers would be able to make choices based on the quality and price of services; and they expect that health plans would compete on quality and price as a result. The problem with this approach is that

---

97 *See* PPRC 1994, *supra* note 10, at 311-12 (listing, in addition to the benefits listed in 1993, the ability to reduce administrative complexity and expenses); PPRC 1993, *supra* note 10, at 33-37 (listing the ability to monitor utilization, costs, and quality of care; to hold providers accountable for quality and access; to support outcomes research and profiling; and to measure risk); PPRC 1992, *supra* note 10, at 263 (listing four objectives of data improvement: administrative efficiency in payment, monitoring the provision and cost of services, profiling, and effectiveness research).

98 *See generally* Paul Starr, *The Framework of Health Care Reform*, 329 NEW ENG. J. MED. 1666 (1993) (discussing President Clinton's Health Security plan).

99 *See* Alain C. Enthoven, *Consumer-Choice Health Plan: A National-Health-Insurance Proposal Based on Regulated Competition in the Private Sector*, 298 NEW ENG. J. MED. 709 (1978); Alain C. Enthoven, *The History and Principles of Managed Competition*, HEALTH AFF., 1993 Supp. at 24; *see also* OTA INFORMATION FOR CONSUMERS, *supra* note 6, at 1 (listing three rationales for the call for more public information).

100 Shoshanna Sofaer, *Informing and Protecting Consumers Under Managed Competition*, HEALTH AFF., 1993 Supp., at 76.

even if a standard benefits package provides consumers with the opportunity to make judgments on the basis of quality, they still lack the information needed to actually assess the quality of health services. Consumers are seldom provided with adequate indicators of the quality of services provided by health plans, hospitals, or health care professionals.[101]

Thus, an effective quality management program must gather better information on quality and must provide consumers with that information in standardized form. A core set of quality and performance measures would assist consumers in making informed health choices. Such information could be provided in annual reports assessing the available health plans according to a series of quality measures, including: (1) access to care (e.g., waiting times to see primary care practitioners and specialists); (2) appropriateness of care (e.g., measured against regional practices or practice guidelines); (3) health outcomes (e.g., percentage of low birth weight infants, nursing home or hospital patients with bedsores, or mortality after a heart attack or stroke); (4) health promotion (e.g., education programs provided such as smoking cessation or stress management classes); (5) disease prevention (e.g., rates for vaccinations, mammograms, prenatal care or HIV screening); and (6) overall satisfaction with care (e.g., percentage of enrollees satisfied with the plan or satisfied with their primary care physician, percentage of enrollees leaving the plan, and the number of complaints filed). Such a program would make it possible for consumers to choose health plans and providers based on standardized performance and satisfaction measures.[102]

---

101 Even under the existing system, some attempt has been made to provide consumers with information about the quality of services. From 1986 to 1993, the Health Care Financing Administration published annual data comparing the mortality experience of hospitals. *See, e.g.*, HEALTH CARE FINANCING ADMINISTRATION, MEDICARE HOSPITAL MORTALITY INFORMATION, 1990 (1991). *See* OTA INFORMATION FOR CONSUMERS, *supra* note 6, at 5. Several states (e.g., California, New York, and Pennsylvania) and voluntary organizations (e.g., the Greater Cleveland Health Quality Choice Project) have published comparative outcome data on health care institutions and professionals. *See, e.g.*, CALIFORNIA OFFICE OF STATEWIDE HEALTH PLANNING & DEV., HEALTH DATA CATALOG (June 1991); CLEVELAND HEALTH QUALITY CHOICE, SUMMARY REPORT (1993) (summarizing for the public information from THE CLEVELAND-AREA HOSPITAL QUALITY OUTCOME MEASUREMENTS AND PATIENT SATISFACTION REPORT (1993)); PENNSYLVANIA HEALTH CARE COST CONTAINMENT COUNCIL, A CONSUMER GUIDE TO CORONARY ARTERY BYPASS GRAFT SURGERY (1992); *see also* HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 96-98; Timothy S. Jost, *Health System Reform: Forward or Backward with Quality Oversight?*, 271 JAMA 1508, 1508-09 (1994); Charles Marwick, *Using High-Quality Providers to Cope with Today's Rising Health Care Costs*, 268 JAMA 2142 (1992).

102 *See* Edward L. Baker et al., *Health Reform and the Health of the Public: Forging Community Health Partnerships*, 272 JAMA 1276, 1280 (1994) (describing the Health Plan Employer Data and Information Set developed by the National Committee for Quality Assurance, a nonprofit accrediting body for managed care organizations, to produce "report cards" for consumers); THE WHITE HOUSE DOMESTIC POL'Y COUNCIL, *supra* note 56, at 111-35.

In the present system, it is virtually impossible to obtain this type of information: there are no requirements for health plans or institutions to maintain data on quality, no standards for uniform data sets to render rational comparisons possible, and no strategies for electronic collection and presentation of these data to consumers. A national information infrastructure could provide consumers with a much broader and more comprehensible range of information, and thus allow them to make more informed choices about health services.

It is reasonable to assume that these innovations would substantially enhance the autonomy and decisionmaking capacity of consumers in the health care system, and that consumer choice would then have some positive effect on quality.[103] Quality assessment is, of course, far more complicated than a "report card" can reflect.[104] A poor outcome measure is not always an indicator of inferior quality; it may just reveal differences in the population of enrollees for the plan. Health plans with low income, sicker populations may score low on performance measures even if they provide high quality services. Moreover, health plans may score relatively well on measures of performance that are included in the report card, but do relatively poorly in areas not included. Plans might "game" the system by channeling resources to measured indicators, while ignoring quality problems in other areas. The result would be high marks on the report card, but otherwise inferior quality services.[105]

Some commentators argue that streamlining the existing regulatory system for overseeing the quality of health services[106] and relying instead on the empowerment of consumers will harm quality rather than enhance it.[107] They suggest that, regardless of the information provided, consumers are ill-equipped to make reasoned judgments

---

103 *See generally* Douglas Sharrott, *Provider-Specific Quality-of-Care Data: A Proposal for Limited Mandatory Disclosure*, 58 BROOK. L. REV. 85 (1992).

104 *See* Jesse Green, *Problems in the Use of Outcome Statistics to Compare Health Care Providers*, 58 BROOK. L. REV. 55 (1992).

105 Gostin, *supra* note 1, at 8.

106 Under the Health Security Act, *supra* note 88, the National Quality Management Program would develop uniform standards for licensing health care institutions that focus on essential performance requirements. However, the Medicare Peer Review Organization would end once the Secretary of Health and Human Services determined that Medicare enrollees were adequately protected through the National Quality Management Program. In addition, the administrative requirements under the Clinical Laboratory Improvements Act would be reduced. *See* WHITE HOUSE DOMESTIC POLICY COUNCIL, *supra* note 56, at 118-22; *see also* Timothy S. Jost, *Administrative Law Issues Involving the Medicare Utilization and Quality Control Review Organization (PRO) Program: Analysis and Recommendations*, 50 OHIO ST. L.J. 1, 51-53 (1989).

107 Jost, *supra* note 106.

about health services.[108] However, although misleading claims of quality and performance often limit rational market decisions, consumers in the health care market can, and should, play the most effective role possible in influencing the price and quality of services. Considerable empirical scholarship is emerging on the value of publicly disclosing information to consumers.[109] Although the value of such disclosure is dependant on the reliability, validity, fairness, and comprehensibility of the data, thoughtful strategies have been suggested to improve the quality of consumer information, meeting many of the objections of critics.[110]

Providing accurate information to consumers that facilitates logical comparisons among plans and providers would result in several broad benefits. First, arming consumers with the most reliable information has intrinsic value in enhancing autonomy and a sense of shared participation in the health services market. Just as the prevailing legal and ethical thought consistently promotes autonomous decisions by patients regarding their treatment,[111] so should consumers be encouraged to make choices about their health plans and providers.[112] Second, public disclosure of information promotes health education. It enables consumers to have a more sophisticated understanding of the health care system as a whole, as well as the costs and quality of individual services. It may also improve understanding of the relationship between personal behavior and health out-

---

108 *See, e.g.*, Timothy S. Jost, *The Necessary and Proper Role of Regulation to Assure the Quality of Health Care*, 25 HOUS. L. REV. 525, 560-64 (1988) (making this argument); *see also* Dent v. West Virginia, 129 U.S. 114, 122-23 (1889) ("Every one may have occasion to consult [the physician], but comparatively few can judge of the qualifications of learning and skill which he possesses. Reliance must be placed upon the assurance given by his license, issued by an authority competent to judge in that respect, that he possesses the requisite qualifications.").

109 *See* HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 91-129; OTA INFORMATION FOR CONSUMERS, *supra* note 6, at 23.

110 The OTA made the following recommendations for disseminating information to consumers: stimulate consumer awareness of quality of care; provide easily understood information; present information in more than one format; use reputable organizations to interpret quality-of-care information; make information accessible; and provide consumers with the skills to use, and physicians the skills to provide, information on quality of care. OTA INFORMATION FOR CONSUMERS, *supra* note 6, at 40-47.

111 *See generally* Lawrence O. Gostin & Robert F. Weir, *Life and Death Choices After Cruzan: Case Law and Standards of Professional Conduct*, 69 MILBANK Q. 143 (1991) (exploring the law, ethics, and professional standards regarding patients' autonomous decisionmaking).

112 Arguably, macro decisions about which plan or hospital to choose have a greater impact on the health of the person than micro decisions about which treatment to choose. Furthermore, arguments about the ability of competent patients to understand treatment options have not caused courts or commentators to abandon the principle of autonomous decisionmaking in the context of treatment decisions. Nor should legal or ethical analysis accept the assertion that consumers simply lack the sufficient sophistication to understand the complexities of the provision of health services. *See* Sharrott, *supra* note 103, at 85-88.

comes.[113] Finally, while managed competition theorists may have overstated their claim that informed consumers will influence the market to provide more cost-effective services, it is likely that providing consumers with reliable and relevant information will ultimately have a positive effect on the market for health services.[114]

2. *Improving the Quality of Health Services*

Empowering consumers to make more informed choices, if it is to be effective in improving quality, must be undertaken in conjunction with several other strategies.[115] These strategies include the setting of minimum standards, the development of practice guidelines, the monitoring of provider performance, and the provision of reliable, complete, and timely information to regulators, health plans, institutions, and health care professionals. A health information infrastructure could increase the effectiveness of each of these strategies for enhancing the quality of health services.

A helpful way of assessing the benefits of a health information infrastructure is to imagine how data, now largely unavailable, could help participants in the health care system improve the quality of patient services. Health care professionals rarely have access to full information about their patients, including their behavioral and clinical history, immunizations, screenings (e.g., mammogram, pap smear, PPD skin test, or HIV antibody test), allergies to medications, diagnostic tests, and treatments.[116] The lack of accurate, comprehensive, and accessible information makes it more difficult, time consuming, and costly to provide a full range of health services to patients. A computerized patient record would enable health care providers to furnish clinical prevention services such as outreach (e.g., tracking children

---

113 The Institute of Medicine concluded that

> the public interest is materially served when society is given as much information on costs, quality, and value for health care dollar expended as can be given accurately and provided with educational materials that aid interpretation of that information. Indeed, public disclosure and public education go hand-in-hand.

HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 95.

114 Many observers believe that one of the principal effects of a health care reform that limits price increases, disallows preexisting condition clauses, and prohibits risk selection will be that competition on the basis of quality of services will become more prominent. HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 73; AMERICAN MEDICAL PEER REVIEW ASS'N, MANAGED COMPETITION AND THE ROLE OF QUALITY OVERSIGHT (1993).

115 OTA INFORMATION FOR CONSUMERS, *supra* note 6, at 28 ("[I]nforming consumers and relying on their subsequent actions should not be viewed as the only method to encourage hospitals and physicians to maintain and improve the quality of their care. Even well-informed lay-people . . . must continue to rely on experts to ensure the quality of providers."); *see also* Alan L. Hillman et al., *Safeguarding Quality in Managed Competition*, HEALTH AFF., 1993 Supp., at 110.

116 For a discussion of the inadequacy and duplication of manual records, see *supra* notes 25-27 and accompanying text.

who have not been immunized) or health promotion (e.g., providing HIV risk prevention for intravenous drug users) far more efficiently.[117]

Computerized records could increase the effectiveness of prevention programs that cannot be conducted without complete information about screening, vaccinations, risk profiles, or other essential data. Computers can also issue reminders to clinicians to perform indicated medical tests. Access to a full patient record is equally valuable in emergency situations or in the management of complex cases. Databases that include prescriptions and sales of pharmaceuticals could help pharmacists and primary care providers to track their proper use among elderly patients or report adverse drug reactions. Genetic databases with complete personal and family histories may become vital for testing, counselling, and treatment of persons with genetic traits, predispositions, or disease.[118]

Effective clinical decisionmaking for health care professionals is influenced not only by the information available about the patient and his or her family, but also the information that is available to assist in the diagnosis and treatment of disease.[119] Health care professionals know surprisingly little about the health outcomes of a large number of standard medical interventions.[120] Frequently, this results from an insufficient amount of research or a lack of scientific consensus about the cost effectiveness of treatments. However, it can also result from practitioners' lack of information. Automated information systems could assist in a number of ways to obtain and disseminate this information to health care professionals. With data from large populations more accessible, outcomes research could better an-

---

117 For example, approximately two fifths of two-year-old children in the United States have not received recommended immunizations on schedule. Gary L. Freed & Samuel L. Katz, *The Comprehensive Childhood Immunization Act of 1993: Toward a More Rational Approach*, 329 NEW ENG. J. MED. 1957 (1993). Some observers think a national or statewide tracking and reminder system (eliminated from President Clinton's childhood immunization initiative) would be an effective strategy for increasing the rate of childhood vaccination. *Id.*; *see also supra* note 72 and accompanying text.

118 *See generally* George Annas, *Privacy Rules for DNA Databanks: Protecting Coded Future Diaries*, 270 JAMA 2346 (1993) (discussing the efficiency of patient databases and privacy issues); Andrea de Gorgey, Note, *The Advent of DNA Databanks: Implications for Informational Privacy*, 16 AM. J.L. & MED. 381 (1990) (discussing possibility of accumulating a massive genetic databank and the privacy concerns that might result from such an undertaking).

119 *See generally* Richard J. Johns & Nicholas J. Fortuin, *Clinical Information and Clinical Problem Solving*, *in* THE PRINCIPLES AND PRACTICE OF MEDICINE 1 (A. McGehee Harvey et al. eds., 22d ed. 1988); Richard J. Johns et al., *The Collection and Evaluation of Clinical Information*, *in id.* at 4.

120 *See* HENRY J. AARON, SERIOUS AND UNSTABLE CONDITION: FINANCING AMERICA'S HEALTH CARE 15-16 (1991); David M. Eddy, *Variations in Physician Practice: The Role of Uncertainty*, HEALTH AFF., Summer 1984, at 74; M. Gregg Bloche, *Managed Care: A Second Opinion*, LEGAL TIMES, Nov. 16, 1992, at 17.

swer important clinical questions;[121] with more easily analyzed data collections, policy makers could more effectively develop minimum standards or practice guidelines;[122] and with user-friendly decision trees available in health care offices and institutions, health care professionals could receive immediate assistance in making complex clinical decisions.

3. *Assessing System Performance*

If the health care system exists to achieve fundamental social goods for the nation, then what are the goods that we wish to achieve, and how can they be measured? The primary goals of the health care system, often stated, are access to services, equitable distribution of services, and cost effectiveness (i.e., ensuring high quality services at a reasonable cost). A health information infrastructure could help the government accurately assess planning, performance, and delivery to determine if these objectives are being achieved.

Persistent and sometimes substantial differences exist in the availability and quality of health care in the United States.[123] Differences occur between the uninsured and the insured,[124] the poor and the rich,[125] those in public (e.g., Medicaid) and private programs,[126] mi-

121 *See infra* notes 140-44 and accompanying text.

122 The National Quality Management Program proposed by the Clinton Administration would develop practice guidelines to assist providers in achieving quality standards and underpin national measures of quality, develop methodology standards for practice guidelines, operate a clearinghouse and dissemination program for guidelines, and disseminate information documenting clinically ineffective procedures and treatments. WHITE HOUSE DOMESTIC POLICY COUNCIL, *supra* note 56, at 118; *see also* INSTITUTE OF MEDICINE, GUIDELINES FOR CLINICAL PRACTICE: FROM DEVELOPMENT TO USE (Marilyn J. Field & Kathleen N. Lohr eds., 1992). The actual utility of practice guidelines to improve clinical decisionmaking, however, is the subject of considerable disagreement. *See* Bloche, *supra* note 120.

123 *See generally* INSTITUTE OF MEDICINE, ACCESS TO HEALTH CARE IN AMERICA (Michael Millman ed., 1993) (examining the relationship between access to health care and factors such as income, race, clinic origin, and location).

124 *See* Paula Braveman et al., *Adverse Outcomes and Lack of Health Insurance Among Newborns in an Eight-County Area of California, 1982-1986*, 321 NEW ENG. J. MED. 508 (1989); Jeffrey J. Stoddard et al., *Health Insurance Status and Ambulatory Care for Children*, 330 NEW ENG. J. MED. 1421 (1994) (uninsured children are more likely than children with insurance to receive no care from physicians for specified conditions).

125 *See* John Z. Ayanian, *Race, Class, and the Quality of Medical Care*, 271 JAMA 1027 (1994); Katherine L. Kahn et al., *Health Care for Black and Poor Hospitalized Medicare Patients*, 271 JAMA 1169 (1994); Paul H. Wise et al., *Racial and Socioeconomic Disparities in Childhood Mortality in Boston*, 313 NEW ENG. J. MED. 360 (1985).

126 *See* Mark B. Wenneker et al., *The Association of Payer With Utilization of Cardiac Procedure in Massachusetts*, 264 JAMA 125 (1990).

nority and white populations,[127] men and women,[128] and those in rural and urban areas.[129] The best extant research in evaluating differential access to health services has relied on government and other databases. National or regional information systems are essential for the purposes of tracking the use (or under use) of services among traditionally under-served populations (e.g., impoverished children and adults, pregnant women, racial minorities, and persons with disabilities), evaluating the reasons for unequal access, and generally planning and administering a complex population-based health system.[130]

A health information infrastructure could provide similar benefits for tracking the cost of services. Although we know much about escalating health care costs in the United States relative to health expenditures in other countries,[131] we know little about where the greatest costs occur in the system or the reasons for the high costs. This hinders the development of effective methods of reducing the costs. A comprehensive electronic system that tracks expenditures on the basis of variables such as geographic region, health plan or insurer, health care provider, and forms of treatment, and compares these

---

127 *See* John Z. Ayanian, *Heart Disease in Black and White*, 329 NEW ENG. J. MED. 656 (1993); Lance B. Becker et al., *Racial Differences in the Incidence of Cardiac Arrest and Subsequent Survival*, 329 NEW ENG. J. MED. 600 (1993); Council on Ethical & Judicial Affairs, *Black-White Disparities in Health Care*, 263 JAMA 2344 (1990); Eric D. Peterson et al., *Racial Variation in Cardiac Procedure Use and Survival Following Acute Myocardial Infarction in the Department of Veterans Affairs*, 271 JAMA 1175 (1994); Jeff Whittle et al., *Good & Lofgren, Racial Differences in the Use of Invasive Cardiovascular Procedures in the Department of Veterans Affairs Medical System*, 329 NEW ENG. J. MED. 621 (1993); *see also* Vernellia R. Randall, *Racist Health Care: Reforming an Unjust Health Care System to Meet the Needs of African Americans*, 3 HEALTH MATRIX 127 (1993).

128 *See* John Z. Ayanian & Arnold M. Epstein, *Differences in the Use of Procedures Between Men and Women Hospitalized for Coronary Health Disease*, 325 NEW ENG. J. MED. 221, 223-25 (1991).

129 *See* Mark Chassin, *Explaining Geographic Variations: The Enthusiasm Hypotheses*, 31 MED. CARE YS37-44 (1993); Mark Chassin et al., *Variations in the Use of Medical and Surgical Services by the Medicare Population*, 314 NEW ENG. J. MED. 285 (1986).

130 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 69-70. The Institute points out, however, that insurers could potentially use information about utilization to devise insurance packages attractive to, or affordable by, only those groups with low utilization patterns. *Id.* at 70.

131 The United States spent more than $666 billion on health care in 1990, approximately 12% of the nation's gross national product. Health care expenditures are projected to reach $1.6 trillion, between 16% and 18% of the gross domestic product, by the end of the decade if effective controls are not instituted. *See* CONGRESSIONAL BUDGET OFFICE, PROJECTIONS OF NATIONAL HEALTH EXPENDITURES 14 tbl.1 (Oct. 1992); Timothy S. Jost & Sandra J. Tanenbaum, *Selling Cost Containment*, 19 AM. J.L. & MED. 95, 96-97 (1993); George J. Scheiber et al., *Health Care Systems in Twenty-Four Nations*, HEALTH AFF., Fall 1991, at 22, 24; Sally T. Sonnenfeld et al., *Projection of National Health Expenditures Through the Year 2000*, HEALTH CARE FIN. REV., Fall 1991, at 1, 4, 22; Louis W. Sullivan, *The Bush Administration's Health Care Plan*, 327 NEW ENG. J. MED. 801, 801 (1992).

data with health outcomes could constructively assess the cost-effectiveness of services in the system.

An effective health care information infrastructure, then, has considerable potential to assist in measuring system performance in critical areas such as access, equity, and cost. By accurately measuring the success of the system on these and other parameters, a sound information infrastructure ought to improve policy making, resource allocation, and strategic planning. As policy and practice adjustments are made in the health care system, they can also be measured against the same criteria. With on-going assessment based on standardized measures of success, it should be possible to achieve continuous improvement in each of the critical areas of the health care system.[132]

4. *Improving Administrative Efficiency*

One of the most persistent criticisms of the health care system is its costly and inefficient bureaucracy.[133] This is partly caused by the extensive array of uncoordinated private and public sources of financing. Processing of claims for reimbursement by an extensive number of third-party payers, each with its own paper forms and bureaucratic requirements, is burdensome and costly. Approximately nineteen to twenty-four percent of health care expenditures is spent on administrative expenses, and a substantial proportion of these administrative expenditures are consumed by claims processing.[134] Moreover, the myriad number of paper forms, copayment, and deductibility requirements are confusing for consumers and time consuming for health care providers.

A health information infrastructure could reduce many of these paperwork burdens by creating databases containing enrollment, financial, and utilization data, based on uniform electronic records of encounters with health care providers and payment claims.[135] Experience with existing electronic systems used by health insurers shows that automation significantly increases the efficiency of billing, reimbursement, claims tracking, remittance reconciliation, and similar

---

132 *See* Donald M. Berwick, *Continuous Improvement as Ideal in Health Care*, 320 NEW ENG. J. MED. 53 (1989); Avedis Donabedian, *The Quality of Care: How Can It Be Assessed?*, 260 JAMA 1743 (1988).

133 The findings included in the Health Security Act assert that "an excessive burden of forms, paperwork, and bureaucratic procedures confuses consumers and overwhelms health care providers" and that "administrative burdens should be reduced." Health Security Act, *supra* note 88, § 2 (1)(C), (E).

134 Steffie Woolhandler & David U. Himmelstein, *The Deteriorating Administrative Efficiency of the U.S. Health Care System*, 324 NEW ENG. J. MED. 1253, 1255-56 (1991). The net costs of private health insurance consumed 14.2% of premiums collected. Katherine R. Levit et al., *National Health Expenditures, 1990*, HEALTH CARE FIN. REV., Fall 1991, at 36-37; *see also* Jost & Tanenbaum, *supra* note 131, 98, 115.

135 WHITE HOUSE DOMESTIC POLICY COUNCIL, *supra* note 56, at 128-30.

business procedures.[136] It is estimated that the use of electronic data interchange on a system-wide level could create substantial economic savings while reducing time consuming paperwork burdens on health care providers.[137] Studies have demonstrated similar savings by introduction of microcomputer workstations for physicians.[138] Automation could also reduce fraud and abuse by carefully tracking providers' reimbursement claims and matching those claims with electronic treatment records.[139]

5. *Facilitating Research*

If the quality of services and the health of patients and populations are the touchstones of a health care system, then research on the determinants, prevalence, prevention, and treatment of injury and disease deserves preeminent attention.[140] Research in the United States is wide-ranging and includes the investigation of clinical decisions made by health care professionals, health services or patterns of practice, behavior or behavior change of individuals and populations, and the distribution and determination of health-related states or events in specified populations.[141]

A health information infrastructure could improve research in a number of ways: it could make research less expensive by reducing the costs of collecting and analyzing secondary data, more trustworthy because of the accuracy of the data, and more generalizable to all segments of the population[142] because of the completeness of the data. Much of the best health related research uses information that is already collected, and does not involve the prospective gathering of

---

136 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 76.

137 WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, at 3.

138 William M. Tierney, et al., *Physician Inpatient Order Writing on Microcomputer Workstations: Effects on Resource Utilization*, 269 JAMA 379, 381-82 (1993) (A network of microcomputer workstations for writing all inpatient orders lowered one hospital's patient charges and hospital costs by an estimated three million dollars and could potentially save tens of billions of dollars nationwide.).

139 *See* OTA FEDERAL GOVERNMENT TECHNOLOGY, *supra* note 6, at 37-66 (utilizing computer matching to detect fraud, waste, and abuse). The Health Security Act would establish a health care fraud and abuse enforcement program with strengthened controls and penalties as well as antifraud standards for electronic media claims. Health Security Act, *supra* note 88, tit. V(E).

140 *See generally* William L. Roper et al., *Effectiveness in Health Care: An Initiative to Evaluate and Improve Medical Practice*, 319 NEW ENG. J. MED. 1197 (1988) (discussing the benefits of having information on health outcomes).

141 *See generally* John M. Last, *Epidemiology and Ethics*, 19 LAW, MED. & HEALTH CARE 166 (1991) (describing the scope and methodology of epidemiology).

142 More complete data would include, for example, more information about women. *See* Venessa Merton, *The Exclusion of Pregnant, Pregnable and Once-Pregnable People (aka Women) from Biomedical Research*, 19 AM. J.L. & MED. 369 (1993).

primary data.[143] These retrospective studies, while they do not use controls or randomization, often involve rigorous design and statistical methods. An expanded health care database would significantly facilitate this important form of research.

A health information infrastructure could also contribute to classic randomized, controlled trials, particularly large-scale clinical trials that study the safety and efficacy of pharmaceuticals and vaccines. For example, it could help determine the incidence or pattern of disease or treatment in the population and assist in designing a sampling frame for the study.[144] In sum, a health information infrastructure could provide significant benefits for clinical, health services, behavioral, and epidemiological research. Improving the quantity and quality of research would increase our ability to provide cost-effective interventions for the prevention and treatment of injury and disease.

6. *Safeguarding the Public Health*

While clinical medicine is focused primarily on the individual patient and the treatment of disease, the focus of public health is on the vitality of the community and prevention of disease.[145] It is not surprising, therefore, that one of the strongest demands for an expanded health care database comes from those concerned with public health (e.g., the U.S. Public Health Service, state and municipal health departments, community-based organizations, epidemiologists, biostatisticians, and academic schools of hygiene and public health).[146]

There is considerable utility in using population-based data to promote the health of the community. These data can help track the incidence, patterns, and trends of injury and disease in popula-

---

143 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 72-73 (citing Fleming et al., *A Decision Analysis of Alternative Treatment Strategies for Clinically Localized Prostate Cancer*, 269 JAMA 2650 (1993) and Grace L. Lu-Yao et al., *An Assessment of Radical Prostatectomy: Time Trends, Geographic Variation, and Outcomes*, 269 JAMA 2633 (1993)).

144 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 72-73.

145 The public health care system, of course, does play an important role in the treatment of individual patients by providing patient-centered clinical prevention services such as pap smears, mammograms, colerectal screening, and vaccinations.

146 *See* INSTITUTE OF MEDICINE, THE FUTURE OF PUBLIC HEALTH App. A (1988); Baker et al., *supra* note 62, at 1281 ("[T]he CDC is vigorously promoting electronic information sharing between state public health agencies and itself, and it is also seeking to stimulate similar connectivity among public health partners within states."); Andrew Friede et al., *CDC Warden: A Comprehensive On-Line Public Health Information System of the Center for Disease Control and Prevention*, 83 AM. J. PUB. HEALTH 1289 (1993) (describing CDC mechanism for placing information in the hands of health care professions).

Government at all levels may have a keen interest in these data. While this discussion focuses primarily on health departments, it is conceivable that the information would be used for health-related purposes by other parts of government, such as those responsible for social services, child protection, welfare, housing, and nutrition.

tions.[147] Carefully planned surveillance or epidemiological activities facilitate rapid identification of health needs, including the spread of communicable or sexually transmitted infection or disease (e.g., HIV, TB, hepatitis B virus, or herpes simplex), clusters or outbreaks of bacterial or viral infection (e.g., Legionnaire's disease, hanta virus, or E. Coli), the initiation of risk behaviors in sub-populations (e.g., smoking among female adolescents or ethnic minorities), and patterns of harm (e.g., child or spousal abuse, lead poisoning, radon, iatrogenic injuries, or gunshot wounds). Tracking of health risks allows those concerned with public health to concentrate resources and focus interventions in areas of greatest need. Well targeted prevention programs such as health education and promotion, testing and counseling, treatment, and contact tracking are highly cost effective.[148]

Health departments do not have the capacity (in terms of laboratories, surveillance, outreach programs, and information systems) to identify and effectively respond to the great variety of health risks facing populations.[149] Surprisingly, health departments have relatively few tools to gather the information about health threats in a timely manner: they do not have the resources to routinely screen for most diseases; many diseases are not reportable or are under reported; and surveillance and epidemiologic research are usually narrowly focused on specific diseases or geographic areas.[150]

Many public health functions are the joint responsibility of the personal health care system and the public health system. Accordingly, reliable information needs to be shared across these two health systems. For example, prevention, diagnosis, and treatment of drug and alcohol dependency, sexually transmitted diseases, AIDS, and tuberculosis are undertaken both by health care providers and health departments. Similarly, registries containing information about immunizations, traumas, and cancers may provide substantial advantages to health care providers and health departments in understanding the determinants of disease (environmental, occupational, or genetic) and outcomes following interventions. Databases containing information about blood types, organs, and tissues could improve the safety,

147 *See, e.g.*, 3 CENTERS FOR DISEASE CONTROL, NATIONAL HIV SEROSURVEILLANCE SUMMARY: RESULTS THROUGH 1992, at 4-5 (1994) (reporting results of HIV prevalence in adolescents, women, adults at high risk for acquiring HIV, and minority populations).

148 *See* Joycelyn Elders, *The Future of U.S. Public Health*, 269 JAMA 2293 (1993) (each dollar spent on prevention saves several dollars in personal medical services).

149 *See* INSTITUTE OF MEDICINE, *supra* note 146, at 19-34; Eugene Feingold, *Health Care Reform—More Than Cost Containment and Universal Access*, 84 AM. J.L. & PUB. HEALTH 727, 727-28 (1994); *see also* WHITE HOUSE DOMESTIC POLICY COUNCIL, *supra* note 56, at 161-69 (public health initiatives).

150 *See* Lawrence O. Gostin, *The Future of Public Health Law*, 12 AM. J.L. & MED. 461 (1986).

efficacy, and efficiency of the blood supply, organ procurement, and transplantation.[151]

Consider, as an illustration, the role of health information in the case of tuberculosis control.[152] Persons with multidrug-resistant tuberculosis frequently come into contact with a wide variety of agencies and organizations, each of which may be unaware that the person is infectious or may not be taking prescribed antituberculosis drugs. Persons with tuberculosis often make multiple appearances in emergency rooms (sometimes under assumed names and at different hospitals); come in and out of jails, prisons, and community corrections (on parole or probation); attend clinics for methadone maintenance or other drug treatment; are temporarily resident in a homeless shelter; and receive diagnostic and treatment services in sexually transmitted disease or HIV clinics.[153] Yet, none of these entities may have ready access to information in the personal health record or tuberculosis registry held by the state public health department. As a result, these individuals, who are under the jurisdiction of health, social services, or corrections authorities, are often not identified and are at considerable risk of spreading the infection in the community or in congregate settings. If the health record or tuberculosis registry were readily available, the spread of the disease could be sharply curtailed.

Personal health services, it must be emphasized, are only a small subset of the range of interventions that contribute to a healthy population. Tracking disease and injury in the population and providing well-targeted prevention services can reduce overall morbidity and mortality in the community more effectively and inexpensively than technologically advanced medical services. By providing public health access to comprehensive data on injuries and diseases within broad populations, society can achieve remarkable benefits for the vitality of the community.[154]

---

151 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 79-81; *see also* Martin Benjamin et al., *What Transplantation Can Teach Us About Health Care Reform*, 330 NEW ENG. J. MED. 858 (1994).

152 *See generally* Lawrence O. Gostin, *The Resurgent Tuberculosis Epidemic in the Era of AIDS: Reflections on Public Health, Law, and Society*, 54 MD. L. REV. 1 (1995).

153 *See* Centers for Disease Control, *Tuberculosis Prevention in Drug-Treatment Centers and Correctional Facilities—Selected U.S. Sites, 1990-1991*, 42 MORBIDITY & MORTALITY WKLY REP. 210 (1993); Centers for Disease Control, *Transmission of Multi-Drug-Resistant Tuberculosis Among Immunocompromised Persons, Correctional System—New York 1991*, 41 MORBIDITY & MORTALITY WKLY REP. 507 (1992); Peter A. Selwyn et al., *A Prospective Study of Tuberculosis Among Intravenous Drug Users with HIV Infection*, 320 NEW ENG. J. MED. 545 (1989); Dixie E. Snider & Mary D. Hutton, *Tuberculosis in Correctional Institutions*, 261 JAMA 436 (1989).

154 *See generally* U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHY PEOPLE 2000: NATIONAL HEALTH PROMOTION AND DISEASE PREVENTION OBJECTIVES (1991) (setting health promotion and disease prevention goals for the United States to achieve by the year 2000, and arguing that prevention is a cost-effective strategy for the nation); Lawrence O. Gostin, *Securing Health or Just Health Care? The Effect of Health Care Reform on the Health of America*, 39

II
INFORMATIONAL PRIVACY WITHIN A HEALTH INFORMATION INFRASTRUCTURE

The vision of a comprehensive health information system described in the previous Part of this Article is technologically feasible, and a well-functioning system of this kind would be likely to achieve significant societal benefits. However, in order to decide whether to build a health information system, it is necessary to measure the probable effects of that system on the privacy of individuals and populations. The diminution in privacy entailed in a comprehensive health information system depends on the number of individuals and organizations that would have access to the data, the sensitive nature of the data to which they would have access, and the enhancing power of automation as a means both to protect and to attack the privacy of patients.

A. The Proliferation of Authorized and Unauthorized Users of Health Data

In order to understand the proliferation of possible users, it is helpful to identify the potential customers for health information. If an entity can demonstrate the social or financial worth of health information, it can probably make a strong claim for access to that information. Potential customers are those who find health information valuable for any number of purposes, ranging from core functions such as clinical decisionmaking, cost containment, quality assessment, and research, to more tangential functions such as employment, insurance, and commerce.

Advocates have long recognized that the most serious threats to privacy come from authorized users of health information.[155] Providing a reasonable measure of privacy for the individual requires, at the very least, some control over the number of individuals that have access to health information. Once large numbers of individuals and organizations have access to sensitive and often highly valuable information, it becomes difficult to prevent uses that stigmatize or harm the subjects of those data.

The Institute of Medicine found that the number of authorized users of the computer-based patient record is too exhaustive to list, and would parallel the complete list of the individuals and organizations associated directly or indirectly with health care: "Patient record

---

ST. LOUIS U. L. REV. 7 (1995) (arguing that improving the health of the community should be the overriding goal of the health care system).

155 *See, e.g.*, WORK GROUP ON COMPUTERIZATION OF PATIENT RECORDS, *supra* note 9, App. D.

users provide, manage, review, or reimburse patient care services; conduct clinical or health services research; educate health care professionals or patients; develop or regulate health care technologies; accredit health care professionals or provider institutions; and make health care policy decisions."[156] The Institute cataloged thirty-three representative individual users of patient records, and thirty-four representative institutional users.[157] Health information users are not limited to those with primary justifications such as health care delivery, patient management, and financial reimbursement. Secondary uses of patient records include education (e.g., conferences, teaching hospitals, and continuing education), regulation (e.g., litigation, postmarketing surveillance, and accreditation), commercialization (e.g., development of biotechnologies and marketing strategies), social services and child protection (e.g., tracking and intervening in spousal or child abuse), and public health (e.g., disease reporting, partner notification, and surveillance).[158]

Since virtually all of the various plans for a health information infrastructure assert a broad range of compelling health objectives,[159] it is likely that Congress or the appropriate regulatory agencies would authorize a large number of individuals and institutions to access patient records. Certainly, Congress or the appropriate agency would attempt to limit authorized users to the relevant portion of the record. However, whether their purpose is clinical, financial, or regulatory, most users would assert a need to know large portions of the record. It is difficult to envisage the development of meaningful controls over the kinds of data authorized individuals could obtain and the uses they would make of those data.[160] For example, even the most pri-

156 INSTITUTE OF MEDICINE, *supra* note 25, at 31.

157 *Id.* at 32-33. Representative individual users include: (1) those concerned with patient delivery such chaplains, dentists, dietitians, lab technologists, occupational therapists, optometrists, and pharmacists; (2) those concerned with patient management such as administrators, accountants, risk managers, and utilization review managers; and (3) those concerned with patient care reimbursement such as benefit managers and governmental and private insurers. Representative institutional users include: (1) entities concerned with health care delivery such as health plans and networks of providers, donor banks, ambulatory surgery centers, hospices, public health departments, and substance abuse programs; (2) entities concerned with review of care such as Medicare peer review organizations, quality assurance companies, and utilization management companies; (3) entities concerned with research such as disease registries, health data organizations, and health care technology developers; (4) entities concerned with education such as schools of medicine, nursing, or public health; (5) entities concerned with accreditation such as professional and institutional licensure agencies; and (6) entities concerned with policymaking such as federal or state government agencies. *Id.*

158 *Id.* at 34-35.

159 *See supra* parts I.D.2 and I.D.3.

160 At the most basic level it would be possible to limit pharmacists to information concerning prescriptions or laboratory technicians to information about test results. Even in these simple cases, however, pharmacists may assert a need to know a broader physical

vacy-oriented bills in Congress provide health care professionals with broad authority to disclose information without the patient's consent for the purposes of treatment, reimbursement for services, oversight, public health, emergencies, legally required reporting, health research, law enforcement, and subpoenas and warrants.[161]

Presumably, authorized users of health information would possess a patient identification number that would grant them access to all or part of the electronic record.[162] The unique identifier would permit entry to many potential data sources held by government agencies, health plans, health data organizations, and other information holders. It follows that physicians, nurses, pharmacists, lab technicians, administrators, payors, regulators, and many others could retrieve a comprehensive health record from any geographic area linked to the health data network. Patients would not consent to access other than in the most general way, and could not realistically govern the manner in which data were utilized.

It is clear, moreover, that individuals and organizations that are not explicitly authorized might also gain access to the information. Powerful commercial reasons exist for obtaiuing access to health information. There is a market for the "sale of personal information from both public and private sources, encouraged by financial incentives for staff to supplement their income through unauthorized disclosures of personal information."[163] Unauthorized access to personal information can be motivated by many factors. These include profiting from the sale of data to information brokers or marketing firms; uncovering sensitive information about famous individuals such as a history of mental illness, HIV infection, or a sexually transmitted disease; possessing information that may be helpful in litigation such as malpractice actions; and using the information to make employment or insurance decisions.

Simply because the collection of information is not specifically authorized does not necessarily render it unlawful. It is possible to

---

and mental history to check for allergies, possible adverse effects, or multiple prescriptions; and lab technicians may claim a need to know additional clinical details such as a person's HIV status for tuberculin skin tests. Members of the multidisciplinary team, health plan managers, third-party payers, and regulators are likely to seek broad access to the entire record. Neither the existing bills in Congress, nor the strategic planning documents recommending a health information infrastructure, significantly limit access to authorized users.

161 *See* Fair Health Information Practices Act of 1994, H.R. 4077, 103 Cong., 2d Sess. (1994). The Bill is intended to be considered as part of the Health Security Act, *supra* note 88.

162 Not all users, of course, would have access to the entire record at all times. Some users would have frequent access to the record, while others would access the record sporadically, and others still would never actually see the record, but would obtain data derived from it. INSTITUTE OF MEDICINE, *supra* note 25, at 31.

163 OTA PROTECTING PRIVACY, *supra* note 6, at 26.

assemble a detailed personal dossier of an individual at very low cost simply by obtaining lawful access to data in commercial and governmental electronic databases.[164] The Krever Commission in Canada[165] and the U.S. Congressional Office of Technology Assessment documented hundreds of successful attempts by private investigative firms, newspapers, and others to acquire information without the consent of patients at relatively little cost.[166]

Additionally, there exists a growing number of health data-base organizations designed to further their own commercial interests. These organizations use their lawful connections to the health care system to collect and sell information, usually without the knowledge or consent of patients.[167] For example, the Medical Information Bureau collects comprehensive health information, and informs its 700 member insurance companies about known actuarial risks of applicants.[168] Similarly, the Physician Computer Network, Inc. collects a broad range of information about financial management, medical records, and office management, and links its 2,000 office-based physicians to hospitals, laboratories, insurers, pharmaceutical companies, and managed-care providers.[169] These, and many other examples of widespread information collection, suggest that as more individuals and organizations gain lawful access to data there are innumerable opportunities to lawfully aggregate, use, and sell the data for purposes that patients never anticipated when the data were originally collected.[170]

Personal information can also be obtained in fraudulent ways. The Office of Technology Assessment (OTA) suggests that the unlawful sale of personal information from data banks held by government or the private sector, particularly medical information, is widespread.

---

164 The computer magazine *Macworld*, for example, obtained a considerable amount of personal information on celebrities through lawful means. The magazine spent an average of $112 and 75 minutes per subject. Charles Piller, *Privacy in Peril, How Computers are Making Private Life a Thing of the Past*, MACWORLD, July 1993, at 127-28.

165 The Royal Commission of Inquiry Into the Confidentiality of Health Records in Ontario Canada (Chaired by Mr. Justice Horace Krever, 1980). *See* OTA PROTECTING PRIVACY, *supra* note 6, at 28 (discussing Krever Commission study).

166 OTA PROTECTING PRIVACY, *supra* note 6, at 23-37.

167 *See* Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1402-03 (1987).

168 OTA PROTECTING PRIVACY, *supra* note 6, at 32-33.

169 *Id.* at 33-35.

170 *See, e.g.*, 1 INDEPENDENT COMM'N AGAINST CORRUPTION, REPORT ON UNAUTHORIZED RELEASE OF GOVERNMENT INFORMATION ix (Aug. 1992) (Australia) (Ian Temby, Commissioner) (finding "widespread corrupt trade" in government information); PRIVACY PROTECTION STUDY COMM'N, *supra* note 13, at 3-6 (advocating a national policy regarding the treatment of computerized records); JEFFREY ROTHFELDER, PRIVACY FOR SALE 31-88 (1992) (discussing the proliferation of information sources available to credit reporting agencies and the case of accessing sensitive information through licit and illicit means); Piller, *supra* note 164, at 127-28 (demonstrating the ready accessibility of personal information).

The OTA provides numerous examples of prosecutions for breaches of privacy against current and former employees of the federal government (e.g., employees of the Social Security Administration and Internal Revenue Service), local police officers accessing the FBI's National Crime Information Center, and private information brokers.[171] There are several primary methods for obtaining unlawful access to personal information: entering into contracts with employees who have access to the information; paying sums of money to outside entities that already have legitimate access such as insurance companies; obtaining the person's social security number and using it to access the computerized record; and pretending to be an authorized user from another office whose computers are down, an activity referred to as "pretexting."[172]

An extensive health information infrastructure, then, creates numerous opportunities for invasion of privacy. The sheer number of authorized users, the potential for lawful access without explicit authority, and the threat of fraudulent access render it virtually impossible to ensure significant levels of privacy for patients under the national information system contemplated.

B. The Sensitive Nature of Health Information and the Harms of Disclosure

The problem for persons concerned with privacy is not simply the almost inexhaustible opportunities for access to data but also the intimate nature of those data, the potential for harm to persons whose privacy is violated, and the overall effect on the health care system if privacy is eroded.

Only a few generations ago, physicians kept minimal written records about their patients. Physicians usually knew their patients and did not see a need to maintain extensive written reminders of patients' clinical histories. Today, the quantity of health records and the nature of the data they contain have increased substantially.[173] The health records of patients, therefore, contain significant amounts of sensitive information that are available for inspection by many others.[174] Modern medicine understands a great deal more about the effects on a patient's physical and mental health of human behavior (e.g., sexuality, smoking, alcohol use, or drug injection and needle sharing), genetic profile (based on family history and genetic testing),

---

171 OTA PROTECTING PRIVACY, *supra* note 6, at 26-29.

172 *Privacy of Social Security Records: Hearing Before the Subcomm. on Social Security and Family Policy of the Senate Comm.*, 102d Cong., 2d Sess. 62-67 (1992) (statement of Larry D. Morey, Deputy Inspector General for Investigations, Department of Health and Human Services), *cited in* OTA PROTECTING PRIVACY, *supra* note 6, at 29.

173 PRIVACY PROTECTION STUDY COMM'N, *supra* note 13, at 277.

174 HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 140.

and social conditions (e.g., poverty, nutrition, and social relationships). Physicians document these and other personal data not only to ensure better treatment and continuity of care but also to protect against allegations of malpractice.

It follows that health records contain a vast amount of personal information with multiple uses: demographic information, such as age, sex, race, and occupation; financial information, such as employment status and income; information about disabilities, special needs, and other eligibility criteria for federal or state subsidies; medical information such as diagnoses, treatments, and disease histories, including mental illness, drug or alcohol dependency, acquired immunodeficiency syndrome, and sexually transmitted diseases; personal and social information such as sexual orientation, family status, sexual relationships, and lifestyle choices; and information about being the subject or perpetrator of violent behavior such as rape, spousal or child abuse, or firearm injuries. This information is frequently sufficient to provide a detailed profile of the individual. Traditional medical records, moreover, are only a subset of records containing substantial health or personal information held by educators, employers, social services, immigration, law enforcement, credit and banking institutions, and many others.

A variety of underlying harms to patients may result from unwanted disclosures of these sensitive health data. Intrinsic harms result from the mere fact of an unwanted or unjustified disclosure of personal information. Many moral views recognize the desirability of protecting individuals against the insult to dignity and the lack of respect for the person evidenced by such disclosures. Furthermore, a breach of privacy can result in economic harms such as loss of employment, insurance, or housing. It can also result in social or psychological harms. Disclosure of some conditions can be stigmatizing, and can cause embarrassment, social isolation, and a loss of self-esteem. These risks are especially great when the perceived causes of the health condition include the use of illegal drugs, socially disfavored forms of sexual expression, or other behavior that triggers social disapproval. Moreover, stigmatization may be a consequence of such disclosures in some instances even when the potential causes do not involve any despised choices or behavior on the part of the affected individual. Family members, neighbors, and work associates may withdraw social support from individuals known to have certain conditions, especially mental or emotional instability, or physical or behavioral attributes that some people find uncomfortable to observe.

Maintaining reasonable levels of privacy is essential to the effective functioning of the health and public health systems. Patients are less likely to divulge sensitive information to health professionals if

they are not assured that their confidences will be respected. The consequence of incomplete information is that patients may not receive adequate diagnosis and treatment of important health conditions. Moreover, failure to divulge communicable conditions such as HIV infection may pose a risk to the health of sexual or needle-sharing partners. Persons at risk of disease may not come forward for the testing, counseling or treatment necessary to protect the public health. Informational privacy, therefore, is valued not only to protect patients' social and economic interests, but also their health and the health of the wider community.

Genomic data present particularly novel and far-reaching privacy concerns, making these data distinct but not unique.[175] The current and likely future proliferation of genetic databases means that holders of these genomic data will possess vast amounts of information.[176] The potential uses of the genetic material are considerable, ranging from clinical, research, and public health applications to determining parentage and providing forensic evidence.

Genomic data can personally identify an individual and his or her bloodline, and provide a more complete profile of current and future health with far more scientific accuracy than other health data. The features of a person revealed by genetic information are fixed—unchanging and unchangeable. Genetic information does not simply reveal important health and personal characteristics of individuals, but also provides important biological facts about their parents, siblings, and children. Genomic data also contain information that is presently indecipherable, but may be unlocked by new scientific understanding.[177] Finally, societies in the past have sought to control the gene pool through eugenics. This becomes particularly worrisome because different genetic characteristics occur with different frequencies in racial and ethnic populations. Although enormous human benefits may accrue from understanding the etiology and pathophysiology of genetic disease, the systematic collection of genomic information holds the potential for grave personal and social detriment.[178]

The combination of emerging computer and genetic technologies poses particularly compelling privacy concerns. Science has the

---

175 *See generally* PRIVACY COMM'R OF CAN., GENETIC TESTING AND PRIVACY (1992) (discussing the threat of genetic identification for personal freedom); E. Donald Shapiro & Michelle Weinberg, *DNA Data Banking: The Dangerous Erosion of Privacy*, 38 CLEV. ST. L. REV. 455, 465 (1990) (discussing privacy concerns regarding DNA profiling); Gorgey, *supra* note 118 (considering the privacy concerns arising from DNA profiling).

176 *See supra* notes 79-82 and accompanying text.

177 Annas, *supra* note 118, at 2346-47.

178 *See* Larry Gostin, *Genetic Discrimination: The Use of Genetically Based Diagnostic and Prognostic Tests by Employers and Insurers*, 17 AM. J.L. & MED. 109, 110-11 (1991); NIH-DOE WORKING GROUP ON ETHICAL, LEGAL, AND SOCIAL IMPLICATIONS OF HUMAN GENOME RESEARCH, GENETIC INFORMATION AND HEALTH INSURANCE (1993).

capacity to store a million fragments of DNA on a silicon microchip. Each DNA chip is loaded with information about human genes. When a component of a patient's blood is placed on the chip, it reveals specific information about the individual's health and genetic composition, potentially ranging from a carrier state (e.g., cystic fibrosis) or a future disease (e.g., Huntington's chorea), to genetic relationships (e.g., establishing paternity or forensic matching of DNA).[179] This technology can markedly facilitate research, screening, and treatment of genetic conditions. But it may also permit a significant reduction in privacy through its capacity to inexpensively store and decipher unimaginable quantities of highly sensitive data.

C. The Enhancing Power of Automation

Automation of health data is frequently presented as an opportunity to *improve* informational privacy.[180] And security measures designed to protect data held in electronic form can be effective: personal identifiers can provide a security key to restrict entry into the information system; information can be organized in levels of increasing security so that users can receive only those data for which they are authorized; health care providers can disclose only the information needed for specific purposes, rather than disclosing a patient's entire medical record; and audits of all individuals who have used the system can help determine if there has been inappropriate or fraudulent access.[181]

Privacy advocates, on the other hand, see computerization as a significant threat to privacy.[182] As vastly greater quantities of informa-

---

179 *See* Ralph T. King, Jr., *Soon, A Chip Will Test Blood for Diseases*, WALL ST. J., Oct. 25, 1994, at B1.

180 *See, e.g., Hearings on Fair Health Information Practices Act of 1994, H.R. 4077 Before the Subcomm. on Information, Justice, Transportation, and Agriculture of the House Comm. on Governmental Operations*, 103d Cong., 2d Sess. (1994) (statement of Nan D. Hunter, Deputy General Counsel, U.S. Department of Health and Human Services) (*available in* LEXIS, Legis. Library, CNGTST file).

181 *See* OTA FEDERAL GOVERNMENT TECHNOLOGY, *supra* note 6, at 37-38; SYSTEM SECURITY STUDY COMM., NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE (1990); OTA DEFENDING SECRETS, *supra* note 59, at 51-91.

182 *See* Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."); *see also* ARTHUR MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); Graham, *supra* note 167, at 1402-05; Arthur Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 1-5 (1972); Arthur Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1107-19 (1969); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1344-48 (1992); John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the U.S.*, 35 HASTINGS L.J. 991, 991 (1984); Project, *Government Information*

tion are collected and transmitted to an ever increasing number of users in remote locations, the ability of consumers to control the dissemination of personal information is sharply reduced.[183] While electronic records are not qualitatively different than manual records, it is much easier to build a personal dossier using automated, on line, and interconnected systems.[184]

Oddly, the claim that computers provide greater security and that they increase the potential for invasion of privacy are both true. Computer security can deter most unauthorized persons from gaining access to the system and can limit the degree of access for authorized users. This can assure significant improvement in security for health information. However, security is never perfect. It will always be possible for determined and sophisticated hackers to gain entry into systems containing huge amounts of personal data.[185] More important, the *raison d'être* of an automated health information system is to make data readily available to a broad range of authorized users. It is the proliferation of these legitimate users of information that pose the greatest risk to informational privacy. No computer security system can control how information is disseminated by individuals and organizations that have legitimate access to data. Increased *security*, then, does not ensure increased *privacy*.[186] Even though advancing technology allows for more rigorous security, automation's potential to make individuals more vulnerable to privacy invasions needs to be faced directly.

Manual records also pose problems of privacy and security, but these problems are less severe than those in the electronic data context. Manual records are often maintained by the health care provider in secure locations with limited numbers of persons having

---

and the Rights of Citizens, 73 MICH. L. REV. 971, 1221-340 (1975); Paul Schwartz, *Administrative Law: The Oversight of Data Protection Law*, 39 AM. J. COMP. L. 618 (1991) (book review).

183 Of course, collection of personal information is not limited to health information. Federal agencies reported that they collected and stored personal information on individuals in approximately 2,000 predominantly computerized systems, principally for the purposes of payment, eligibility, and investigations. GEN. ACCOUNTING OFFICE, COMPUTERS AND PRIVACY: HOW GOVERNMENT OBTAINS, VERIFIES, USES, AND PROTECTS PERSONAL DATA, GAO/IMTEC-90-70BR, 10, 16 (1990).

184 *See* HEALTH DATA IN THE INFORMATION AGE, *supra* note 8, at 136-42; OTA PROTECTING PRIVACY, *supra* note 6, at 23-37; WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 2 at 3-4.

185 *See, e.g.*, Evan Hendricks, *Hacker "Manual" Tells Wannabes How to Penetrate TRW Database*, PRIVACY TIMES July 30, 1992, at 1-2 (reporting the electronic publication of instructions for accessing consumer credit databases).

186 Security and privacy are distinct and separable concepts. Privacy, although a highly complex concept, is defined as the right of an individual to limit access by others to some aspect of the person. *See supra* note 18. Security encompasses a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction and to safeguard the system itself. Security measures alone do not assure protection of privacy.

physical access. The cumbersome nature of manual records makes it an arduous task to acquire, copy, and use them. The relevant data may be held in many different records in diverse locations, making it difficult to combine data from separate sources.

By contrast, computerization makes it easy to enter, transmit, copy, or delete vast amounts of data. The acquisition and dissemination of information is efficient, rapid, and silent. In an electronic, online system, the data can be viewed, studied, and downloaded from any location. The viewer of the information has not acquired any physical materials, making any theft virtually undetectable. Moreover, the viewer of electronic data is not restricted to one set of records but can access many records in diverse geographic locations and databases. This linking capacity allows aggregation, comparisons and matching of data to discover much more about the private lives of patients. Thus, even data that have no personal identifiers may be linked to other data that provide a picture of an identifiable person or population. The linking capacity of computers also enables health database organizations to select characteristics of types of individuals, and to determine the probabilities of such individuals engaging in activities or behavior of interest to the organization. This use of "computer profiling" could, for example, be used to identify individuals who pose a risk to themselves or others due to communicable or sexually transmitted diseases or the failure to take medication.[187]

Computerization allows patient records to be continually updated as new information is added from an abundant number of sources. Thus, continually changing, updated, reconfigured, and manipulated information of vast quantity will be instantaneously available to an indefinable number of users in doctors' offices, health plans, hospitals, and insurance offices—across the state, the country and, quite probably, internationally. The rapid and sophisticated ways that data can be changed and configured, together with the absence of any discrete geographic boundaries for dissemination, provide a dilemma of new dimension for protecting informational privacy.

III

LEGAL PROTECTION OF HEALTH INFORMATIONAL PRIVACY

If society truly believes that the utility of health information warrants building automated and linked systems, it must reckon with the potential diminution in privacy. One method of affording some measure of privacy protection to patients would be to furnish rigorous legal safeguards. However, as this Part demonstrates, the existing

187 *See* OTA FEDERAL GOVERNMENT TECHNOLOGY, *supra* note 6, at 87-95 (finding that the government engages in extensive computer profiling, defined as searching a record system for a specified combination of data elements, i.e., the profile).

legal safeguards are inadequate: Current privacy protection is fragmented and inconsistent, with major gaps in coverage, and there are significant theoretical problems with its structure.[188]

A. Constitutional Right to Informational Privacy

A considerable literature has emerged on the existence and extent of a constitutional right to informational privacy independent of the Fourth Amendment prohibition on unreasonable searches and seizures.[189] To some, judicial recognition of a constitutional right to informational privacy is particularly important since the government is the principal collector and disseminator of information. Citizens, it is argned, should not have to rely on the government choosing to protect their privacy interests. Rather, individuals need protection from the government itself, and an effective constitutional remedy is the surest method to shield them from unauthorized government acquisition or disclosure of personal information.[190] The problem with this approach is that the Constitution does not expressly provide a right to privacy, and the Supreme Court has curtailed constitutional protection both for decisional and informational privacy.[191]

Notwithstanding the Court's current retreat, a body of case law does suggest judicial recognition of a limited right to informational privacy as a liberty interest within the Fifth and Fourteenth Amendments to the Constitution. In *Whalen v. Roe*,[192] the Supreme Court squarely faced the question of whether the constitutional right to privacy encompasses the collection, storage, and dissemination of health information in government data banks.[193] At issue was a New York statute requiring physicians to disclose to the state information about

188 WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 4 at iii (The myriad federal and state laws on health information privacy defy easy categorization. "The result: a morass of erratic law, both statutory and judicial, defining the provider's confidentiality obligation.").

189 *See* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990); Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133 (1991); Heyward C. Hosch III, Note, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis*, 36 VAND. L. REV. 139 (1983).

190 Chlapowski, *supra* note 189, at 134.

191 *See, e.g.*, Webster v. Reproductive Health Servs., 492 U.S. 490 (1989); Bowers v. Hardwick, 478 U.S. 186 (1986); Paul v. Davis, 424 U.S. 693 (1976).

192 429 U.S. 589 (1977).

193 More than a decade prior to *Whalen*, the Ninth Circuit found that police action in distributing a nude photograph of a woman without her consent could constitute "an arbitrary intrusion upon the security of her privacy, as guaranteed to her by the Due Process Clause of the Fourteenth Amendment." York v. Story, 324 F.2d 450, 456 (9th Cir. 1963). Subsequently, the Ninth Circuit limited *York* to its facts. Baker v. Howard, 419 F.2d 376, 377 (9th Cir. 1969).

prescriptions for certain drugs with a high potential for abuse and providing for the storage of those data in a central computer. In dicta, the Court acknowledged "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[194]

However, the Court hardly crafted a constitutional remedy adequate to meet this threat. Justice Stevens, writing for a unanimous court, simply recognized that "in some circumstances" the duty to avoid unwarranted disclosures "arguably has its roots in the Constitution."[195] The Court found no violation in *Whalen* because the state had adequate standards and procedures for protecting the privacy of sensitive medical information. The Court observed that the Health Department carefully gnarded data on dangerous prescription drugs: computer tapes were kept in a locked cabinet; the computer was run off line to avoid accessibility by others; and the information was only disclosed to a limited number of officials.[196] The decision in *Whalen* does little to ensure that future courts will hold health officials to exacting constitutional standards to protect privacy. Rather, the Court suggested deferentially that the supervision of public health and other important government activities "require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[197]

In *Nixon v. Administrator of General Services*,[198] decided four months after *Whalen*, the Court also hesitantly acknowledged a narrow right to privacy.[199] The former President of the United States challenged the constitutionality of a statute directing the Administrator of the General Services Administration to take custody of Presidential materials and to have them screened by federal archivists. The Court recognized that the former President had a legitimate expectation of privacy in his personal communications. However, it upheld the constitutionality of the statute due to the limited intrusion of the screening process, the appellant's status as a public figure, his lack of expectation of privacy in the overwhelming majority of materials, and the virtual impossibility of segregating the small quantity of private materials without comprehensive screening. The Court also empha-

194 429 U.S. at 605.

195 *Id.*

196 *Id.* at 593-94.

197 *Id.* at 605.

198 433 U.S. 425 (1977).

199 *See also* Planned Parenthood v. Danforth, 428 U.S. 52, 80 (1976) (appearing to recognize an independent right to informational privacy, but upholding reporting and record-keeping requirements that were reasonably directed to the preservation of maternal health and properly respected a patient's confidentiality).

sized the statute's sensitivity to legitimate privacy interests and the unblemished record of the archivists for discretion.[200]

Most lower courts have read *Whalen* and *Nixon* as affording a tightly circumscribed right to informational privacy,[201] or have grounded the right on state constitutional provisions.[202] Courts have employed a flexible test balancing the government invasion of privacy[203] against the strength of the government interest.[204] For example, the Third Circuit in *United States v. Westinghouse Electric Corp.*[205] enunciated five factors to be balanced in determining the scope of the constitutional right to informational privacy: (1) the type of record and the information it contains, (2) the potential for harm in any unauthorized disclosure, (3) the injury from disclosure to the relationship in which the record was generated, (4) the adequacy of safeguards to prevent nonconsensual disclosure, and (5) the degree of need for access—i.e., a recoguizable public interest.[206]

Judicial deference to government's expressed need to acquire and use information is an unmistakable theme running through the case law. Provided the government articulates a valid societal purpose[207] and employs reasonable security measures, courts have not interfered with traditional governmental activities of information collection.

---

200 433 U.S. at 465.

201 *But see* J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (holding that the right to privacy does not extend to a general right to nondisclosure of personal information). The Sixth Circuit relied on Paul v. Davis, 424 U.S. 693 (1976) in rejecting a constitutional right to informational privacy. In *Paul v. Davis*, the Supreme Court held that publication by the police department of the fact that a person was arrested for shoplifting did not raise a constitutional question, relying, in part, on the fact that there was no constitutional bar to government publishing a record of an official act such as an arrest. 424 U.S. at 713.

202 *See* People v. Stritzinger, 668 P.2d 738, 742 (Cal. 1983); Falcon v. Alaska Pub. Offices Comm'n, 570 P.2d 469, 476 (Alaska 1977). Some courts have found a right to informational privacy in both the state and federal constitutions. Rasmussen v. South Fla. Blood Serv., Inc., 500 So. 2d 533 (Fla. 1987). *Rasmussen* is the most prominent of many cases addressing informational privacy after courts are asked to compel disclosure of health information through subpoena.

203 The greater the government efforts to avoid nonconsensual disclosure, the weaker the individual's privacy interest.

204 *See Nixon*, 433 U.S. at 458 ("[A]ny intrusion must be weighed against the public interest in subjecting the Presidential materials . . . to archival screening.").

205 638 F.2d 570 (3d Cir. 1980).

206 *Id.* at 578. The Third Circuit used the *Westinghouse* factors in *In re* Search Warrant (Sealed), 810 F.2d 67, 71-72 (3d Cir. 1987).

207 *See, e.g., Westinghouse*, 638 F.2d at 578-79 (noting strong public interest in facilitating research and investigations of National Institute for Occupational Safety and Health); Barry v. City of New York, 712 F.2d 1554, 1560 (2d Cir. 1983) (finding city's financial disclosure law furthered a substantial state interest in deterring corruption and conflicts of interest); Schacter v. Whalen, 581 F.2d 35, 37 (2d Cir. 1978) (finding information crucial to implementation of sound state policy of investigating licensed physicians for medical misconduct).

The right to privacy under the Constitution is, of course, limited to state action. Since the 1970s, more than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests, including limitations on access to personal information.[208] Because most of the state constitutional provisions only protect against breaches of privacy by government,[209] the usual state action limitation renders constitutional claims uncertain. As long as the federal or state government itself collects information or requires other entities to collect it, state action will not be a central obstacle. However, several versions of a health information infrastructure envisage private or quasi-private health data organizations, health plans, and insurers collecting a great deal of information.[210] In these cases, the applicability of constitutional privacy protection would remain in doubt, particularly if database organizations were essentially unregulated by government.

Even in cases where government unambiguously is the collector of data, constitutional limitations may be nominal at best.[211] Courts allow states wide latitude in protecting the public health,[212] and courts are certain to see government purposes of quality assurance, cost containment, or research as substantial, if not compelling. Since policy development on health information pays some attention to privacy and security concerns, the government is likely to prevail on a flexible balancing approach.[213] Absent an improbable upward shift in the courts' level of scrutiny, issues of health informational privacy will be settled in the legislative and executive branches of government.

---

208 ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 17-18 (1981).

209 *See, e.g.*, Rasmussen v. South Fla. Blood Serv. Inc., 500 So. 2d 533, 536 (Fla. 1987); Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 83 (Ct. App. 1991).

210 *See supra* notes 62-78 and accompanying text.

211 Individuals asserting a constitutional right to informational privacy are unlikely to obtain a remedy save in cases where the state fails to assert any significant interest or is particularly careless in disclosing highly sensitive information. *See* Doe v. Borough of Barrington, 729 F. Supp. 376 (D.N.J. 1990) (holding that police officer violated constitutional right to privacy by disclosing that a person was infected with HIV); Woods v. White, 689 F. Supp. 874 (W.D. Wis. 1988) (extending constitutional right to privacy to disclosure of prisoner's HIV status by prison medical service personnel), *aff'd*, 899 F.2d 17 (7th Cir. 1990); Carter v. Broadlawns Medical Ctr., 667 F. Supp. 1269 (S.D. Iowa 1987) (holding that giving chaplains open access to patient medical records violated privacy rights of patients), *cert. denied*, 489 U.S. 1096 (1989).

212 *See* Jacobson v. Massachusetts, 197 U.S. 11 (1905); *see also* Lawrence O. Gostin, *The Americans with Disabilities Act and the Corpus of Anti-Discrimination Law: A Force for Change in the Future of Public Health Regulation*, 3 HEALTH MATRIX 89, 91-103 (1993).

213 One thoughtful commentator has argued that, even if constitutional claims of informational privacy are likely to lose, a significant value to consumers remains, because an ad hoc balancing approach compels government officials to consider privacy when constructing government policies and operating procedures. Kreimer, *supra* note 189, at 147.

B. Legislative and Regulatory Protection of Informational Privacy

Legislatures and agencies have designed a growing number of statutes and regnlations to protect privacy in a developing information society.[214] Legislative and regulatory protection comes in at least six forms: (1) the Privacy Act,[215] (2) the Freedom of Information Act,[216] (3) drug and alcohol privacy regulations,[217] (4) research regulations, (5) confidentiality assurances,[218] and (6) state privacy legislation.[219]

1. *Privacy Act*

The federal Privacy Act of 1974[220] is designed to ensure that federal agencies[221] utilize fair information practices with regard to the collection, use, or dissemination of "any record"[222] which is contained

214 For a discussion of federal privacy statutes that apply primarily outside of the health system (e.g., the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1988); the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1988); and the Electronic Communications Privacy Act, 18 U.S.C. § 2510(5) (1988)), see RICHARD C. TURKINGTON ET AL., PRIVACY: CASES AND MATERIALS 341-51 (1992).

215 *See infra* part III.A.1.

216 *See infra* part III.A.2.

217 *See infra* part III.A.3.

218 *See infra* part III.A.4.

219 *See infra* part III.A.5. Other federal statutes protecting health informational privacy are: (1) the Social Security Act, 42 U.S.C. § 1106 (1988), which prohibits disclosure of any file, record, or other information obtained by officers or employees of the Department of Health and Human Services or its contractors, except as prescribed by regulation (42 C.F.R. § 401.101-.152 (1994)); and (2) the Americans with Disabilities Act, 42 U.S.C. § 12112(c) (1988), which requires that the results of employment entrance and post-employment examinations and inquiries be maintained in separate medical files, and be treated as confidential medical records.

220 5 U.S.C. § 552(b)(1)-(3), (6) (1988).

221 "Agency" is defined to include any executive department, military department, government corporation, or other establishment in the executive branch of government (including the Executive Office of the President), or any independent regulatory commission. 5 U.S.C. § 552(f) (1988).

222 A "record" is "any item, collection, or grouping of identifiable information about an individual maintained by an agency, including . . . his medical history . . . ." 5 U.S.C. § 552a(a)(4) (1988). The definition is broad and includes most forms of data about an individual, including videotapes. *See* Albright v. United States, 631 F.2d 915 (D.C. Cir. 1980).

in "a system of records."[223] First, subject to a number of exceptions,[224] the Act prohibits agencies from disclosing information to any person or to another agency without the prior written consent of the individual to whom the record pertains.[225] Second, each agency that maintains a system of records must also, upon request, permit the individual to review and copy the record.[226] Third, the Act provides a procedure by which an individual may request the correction or amendment of the record.[227] Finally, the Act requires agencies to maintain in their records only personal information that is relevant and necessary to accomplish the agency's purpose.[228] The Computer Matching and Privacy Protection Act of 1988, which amends the Privacy Act, regulates the practice of "matching" files pertaining to the same person through the use of a personal identifier.[229]

Hospitals operated by the federal government and health care or research institutions operated pursuant to federal contract must maintain patient records in compliance with the Act. For example, hospitals that maintain registers of cancer patients pursuant to a federal contract are subject to the Act.[230] The application of the Privacy Act in an evolving health information infrastructure is less certain. To the extent that data are collected by a federal agency such as the Department of Health and Human Services or a special agency within the executive branch, the provisions of the Privacy Act would apply. The

---

223 A "system of records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or other identifiable characteristic. 5 U.S.C. § 552a(a)(5) (1988). Data held by an agency that are not part of a system of records are not protected by the Act—for example, informal memoranda or personal notes about an individual which are not retrievable from a record system. *See* Johnston v. Horne, 875 F.2d 1415, 1423 (9th Cir. 1989) (Supervisor's private notes are not generally subject to requirements of Privacy Act, unless agency uses them to make decisions that concern person's employment status); Smiertka v. United States Dep't of Treasury, Internal Revenue Service, 447 F. Supp. 221, 228 (D.D.C. 1978) (daily reports by agency investigator containing reference to investigation of employee are not subject to requirements of Privacy Act); Savarese v. U.S. Dep't of Health, Educ. & Welfare, 479 F. Supp. 304, 307 (N.D. Ga. 1979) (holding that where files are not keyed for retrieval, information concerning former officer taken from files is not part of system of records and thus is not subject to Privacy Act), *aff'd sub nom.* Savarese v. Harris, 620 F.2d 298 (5th Cir. 1980), *cert. denied*, 449 U.S. 1078 (1981).

224 Agencies may disclose records (1) to agency employees who need the record for the performance of their duties, (2) for "routine" use, (3) to the Bureau of the Census, (4) to recipients for statistical research or reporting if the record is unidentifiable, (5) to the National Archives, (6) to another agency for civil or criminal law enforcement, (7) to a person showing compelling circumstances affecting health or safety, (8) to Congress, (9) to the Comptroller General, pursuant to a court order, or (10) to a consumer reporting agency. 5 U.S.C. § 552a(b)(1)-(12) (1988).

225 *Id.* § 552a(b).

226 *Id.* § 552a(d)(1).

227 *Id.* § 552a(d)(2)-(4).

228 *Id.* § 552a(e).

229 *Id.* § 552a(o).

230 OTA PROTECTING PRIVACY, *supra* note 6, at 42.

Act, however, does not apply to the vast majority of entities that collect health information outside of the federal government.[231]

Even agencies that collect information within the purview of the Act may circumvent its essential purposes. Agencies may disclose information for "routine uses," meaning that they can use health records for any "purpose which is compatible with the purpose for which [the information] was collected."[232] Health agencies have used this concept to justify many further uses of personally identifiable information.[233] For example, the Health Care Financing Administration (HCFA) has a policy of releasing to researchers data collected from patient records by Medicare Peer Review Organizations and stored in the Uniform Clinical Data Set, with patient names and provider identifiers intact.[234] HCFA argues that the disclosure is consistent with the "routine uses" provisions of the Privacy Act because research is compatible with the agency's purpose for collecting the data. While courts might reject HCFA's interpretation, it suggests that the Privacy Act may not be an effective shield against disclosure of personal information by the government.[235]

2. *Freedom of Information Act*

In enacting the Privacy Act, Congress did not seek to interfere with the right of the public to obtain access to information in federal agency records under the Freedom of Information Act of 1966 (FOIA).[236] Accordingly, information that is required to be disclosed under FOIA has no protection under the Privacy Act.[237] The FOIA contains nine exemptions to this rule that permit agencies to withhold disclosure.[238] Exemption 3,[239] which covers data specifically excluded from FOIA disclosure requirements by statute, has been utilized extensively by the Department of Health and Human Services and other agencies to protect health data.[240]

---

231 *See* Gilbreath v. Guadalupe Hosp. Found. Inc., 5 F.3d 785 (5th Cir. 1993) (holding that release of medical records of federal employee's wife and son would not violate Privacy Act because hospitals are not "agencies" of federal government.).

232 5 U.S.C. § 552a(a)(7) (1988).

233 OTA PROTECTING PRIVACY, *supra* note 6, at 41 n.39.

234 Notice of New System of Records, 56 Fed. Reg. 67,078 (1991).

235 *See* WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 4 at 8-9.

236 5 U.S.C. § 552 (1988).

237 *Id.* § 552a(b)(2).

238 *Id.* § 552(b).

239 *Id.* § 552(b)(3).

240 *See, e.g.*, 13 U.S.C. § 9 (1988 & Supp. V 1993) (Department of Commerce raw census data); 42 U.S.C. § 290dd-2 (Supp. V 1993) (Department of Health and Human Services drug abuse patient records); 38 U.S.C. § 5701 (Supp. V 1993) (Veterans' Administration claimants' medical and insurance records); 38 U.S.C. § 5705 (Supp. V 1993) (Veterans' Administration Department of Medicine peer review and quality assurance documents); 42 U.S.C. § 242m(d) (Supp. V 1993) (Department of Health and Human Services identifiable

Exemption 4 concerns "privileged or confidential" data.[241] Federal health agencies, such as the Centers for Disease Control and Prevention, have sought to rely on this exemption to resist discovery of confidential patient or research records in cases such as those involving toxic shock, Reyes syndrome, and cancer registry data.[242] The prevailing judicial view, however, is that information that is privileged from disclosure under the FOIA may nevertheless be subject to discovery.[243] Courts use Rule 26 of the Federal Rules of Civil Procedure to determine the scope of permissible discovery in civil litigation.[244] The courts balance privacy interests of individuals whose identities may be disclosed in the litigation against the parties' interests in the administration of justice; Rule 26 allows the courts to fashion creative protective orders that permit necessary discovery while limiting infringements on privacy.[245]

Exemption 6[246] protects "personnel and medical files and similar files the disclosures of which would constitute a clearly unwarranted invasion of personal privacy."[247] The Supreme Court has adopted a broad construction of this exemption, allowing federal agencies to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information.[248] When an FOIA disclosure is sought from personally identifiable government records, a court must determine whether release of the information would constitute a clearly unwarranted invasion of privacy by balancing the individual's privacy interest with the public's interest in the information.[249]

Although FOIA exemptions can be useful in protecting personal data, they suffer from several limitations. Assuming the data come within one of the listed exemptions, the agency itself has the discre-

---

health statistics); 38 U.S.C. § 7332 (Supp. V 1993) (Veterans' Administration drug abuse, alcoholism, and sickle cell patient records); 42 U.S.C. § 247c(e)(5) (Supp. V 1993) (Department of Health and Human Services venereal disease records).

241 5 U.S.C. § 552(b)(4) (1988).

242 Washington Post v. U.S. Dep't of Health & Human Servs., 690 F.2d 252, 258 (D.C. Cir. 1982).

243 *Id.*

244 Unless limited by court order, "[p]arties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter in the [litigation]." FED. R. CIV. P. 26(b)(1). Determinations as to whether a privilege exists is governed by state law. FED. R. EVID. 501.

245 *See* Lampshire v. Procter & Gamble Co., 94 F.R.D. 58, 60 (N.D. Ga. 1982); Farnsworth v. Procter & Gamble Co., 101 F.R.D. 355, 358 (N.D. Ga. 1984), *aff'd*, 758 F.2d 1545 (11th Cir. 1985); Rasmussen v. South Fla. Blood Serv. Inc., 500 So. 2d 533 (Fla. 1987).

246 5 U.S.C. § 552(b)(6) (1988).

247 *Id.*

248 U.S. Dep't of State v. Washington Post, 456 U.S. 595, 599 (1982) (citing H.R. REP. No. 1497, 89th Cong., 2d Sess. 11 (1966)).

249 Department of the Air Force v. Rose, 425 U.S. 352, 370-76 (1976).

tion, not a duty, to withhold disclosure.[250] Further, the judgment of the agency is subject to judicial review under an unpredictable balancing test that is not always favorable to the individual's assertion of privacy.[251] Accordingly, health care, epidemiological, or research data held by an agency is not assured protection from an FOIA disclosure request or from discovery in civil litigation.

3. *Drug and Alcohol Treatment Records*

Federal law prescribes special privacy rules for the records of patients receiving care for drug or alcohol dependency in federally funded facilities.[252] Strict confidentiality rules apply to oral and written communications of "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance" of any educational, rehabilitative, research, training, or treatment program relating to drug or alcohol abuse.[253] The confidentiality rules apply to any program or activity conducted, regulated, or directly or indirectly assisted by a federal agency. Subject to certain exceptions,[254] the content of a drug or alcohol treatment record can be disclosed only with the consent of the patient.[255]

These disease-specific confidentiality statutes create inconsistencies in the rules governing dissemination of information. Different standards apply to data held by the same federally assisted institutions depending on whether the patient is receiving treatment for substance abuse or some other disease. Furthermore, information about drug and alcohol abuse entered into medical records in nonfederally funded facilities is not protected. Overly strict confidentiality rules could also impede the dissemination of data relating to drug or alcohol dependency treatment for valid purposes such as billing or public health.[256] The creation of strict disease-specific standards so much restrains the dissemination of data in some systems that legitimate health goals are undermined, while other categories of data receive insufficient protection. Any argument that drug and alcohol abuse data deserve special protection rests on a weak foundation because many other health conditions raise similar issues of sensitivity and inti-

---

250 Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979).

251 *See, e.g.*, United States v. Providence Hosp., 507 F. Supp. 519 (E.D. Mich. 1981) (upholding IRS subpoena of hospital substance abuse records).

252 42 U.S.C. § 290dd-2 (Supp. V 1993).

253 42 C.F.R. § 2.1 (1993) (citing 42 U.S.C. § 290ee-3 (1988), which has been incorporated into 42 U.S.C. § 290dd-2 (1988 & Supp. V 1993)).

254 Patient records can be disclosed without consent for medical emergencies; scientific research, audits, or program evaluations; and by court order for good cause. 42 U.S.C. § 290dd-2(b) (Supp. V 1993).

255 The consent must meet the requirements prescribed by regulation. *See* 42 C.F.R. § 2.31 (1993).

256 *See* WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 4 at 10.

macy (e.g., HIV infection, STDs, genetic conditions, and mental illnesses). Indeed, carving out special legal protection for especially sensitive data is inherently faulty, because the desired scope of privacy encompassing a health condition varies from individual to individual. Some patients may be just as sensitive about prevalent diseases such as cancer, heart disease, and diabetes as those diseases selected by legislators to receive "special" protection.[257]

4. *Research Regulations*

Human subject research which is conducted or supported by a federal department or agency must comply with regulations designed to protect human subjects.[258] Among other requirements, applicable research must be approved by a validly constituted Institutional Review Board (IRB). One of the conditions of approval by the IRB is that "[w]hen appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."[259] Furthermore, except where provided in the rules, no investigator may engage a human being as a subject without first obtaining legally effective informed consent. In seeking informed consent, the investigator must provide the subject with "[a] statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained."[260]

Significant gaps in the protection of data about research subjects are apparent. Although the rules apply to research funded by the federal government, private research remains unregulated. Moreover, several categories of research are exempt from the regulations, including investigations involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or non-identifiable.[261] Genetic data bases are especially problematic because they are often termed non-identifiable despite the existence of technology that can link genomic data to a unique individual.

There is considerable variation in the rigor with which IRBs review research studies.[262] Even if IRBs do take confidentiality concerns seriously, the regulations themselves merely require safeguards when "appropriate." Although subjects must be informed whether or not their data is to be held confidentially, the regulations allow investigators to provide no protection, provided the subject consents. Given

257 *See infra* part III.B.6.ii.

258 Protection of Human Subjects, 45 C.F.R. §§ 46.101-.404 (1993).

259 *Id.* § 46.111(a)(7).

260 *Id.* § 46.116(a)(5).

261 *Id.* § 46.101(b)(4).

262 *See* Jay Katz, *Human Experimentation and Human Rights*, 38 ST. LOUIS U. L.J. 7, 14 (1993).

the acknowledged vulnerability of research subjects, the apparent toleration of the waiver of confidentiality in the regulations may not be justified.

Even if the subject provides informed consent to use personal data for the particular research purposes, there is no clear explication in the regulations of further uses that may be made of the data. The original investigator may disclose personal data to other researchers, regulators, and others for related or nonrelated purposes. The data may be given to others in an anonymous form, presumably exempt from the federal regulations. Yet, human subjects may feel violated if they provide consent for research on breast cancer, for instance, and their tissue is later used as part of a genetic data base to identify rare cell lines. Since research is one of the primary justifications for acquisition and use of data, the need for clearer and more comprehensive protection is apparent.

5. *Confidentiality Assurances*

Under section 301(d) of the Public Health Service Act[263] the Secretary may authorize persons engaged in biomedical, behavioral, clinical, or other research to protect the privacy of research subjects by withholding their names or other identifying characteristics from all persons not connected with the conduct of the research.[264] Persons authorized to protect the privacy of research subjects cannot be compelled in any civil, criminal, administrative, legislative or other proceeding to identify research subjects.[265]

---

263 42 U.S.C. § 241(d) (1988).

264 *Id.* The origins of confidentiality assurances date back to the drug war of the 1970s. *See* Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, 84 Stat. 1236 (for drug abuse research). The Attorney General was given a similar authority to "authorize persons engaged in research to withhold the names and other identifying characteristics of . . . subjects." *See* Controlled Substances Act, 21 U.S.C. § 872(c) (1988); *see also* 21 C.F.R. § 1316.23 (1994) (The confidentiality assurance is administered by the Drug Enforcement Administration and is available only for research related to enforcement of laws relating to drugs.). Confidentiality assurances were expanded to cover research on "mental health, including research on the use and effect of alcohol and other psychoactive drugs" in 1974. Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act Amendments of 1974, Pub. L. No. 93-282, 88 Stat. 125. In 1988, confidentiality assurances were expanded to cover health research more generally, in the context of HIV infection and AIDS research.

Research funded by the Department of Justice under the Omnibus Crime Control and Safe Streets Act of 1968, § 812, is subject to built-in confidentiality protection. 42 U.S.C. § 3789g (1988). Confidentiality protection, however, does not apply to the disclosure of future criminal conduct. Additionally, state laws may provide protection. *See, e.g.*, MINN. STAT. ANN. § 144.053 (West 1989); MICH. COMP. LAWS ANN. § 333.2631 (West 1993). Some states have authority similar to federal confidentiality certificate provisions. *See* N.M. STAT. ANN. § 30-31-40 (Michie 1989).

265 Research on mental health or drug or alcohol abuse that is administered by certain agencies of the Department of Health and Human Services is subject to 42 C.F.R. §§ 2a.1-.5 (1992). *See supra* notes 257-61 and accompanying text.

Protection is available upon application from a named project and is conferred in the form of a "certificate of confidentiality" issued directly by the Assistant Secretary for Health.[266] The certificate provides legal authority to resist compulsory demands for identifiable research subject information.[267] An investigator with a certificate has a legal defense against subpoena or court order similar to the physician-patient privilege.[268] The defense applies only to information about individual subjects, not aggregate data.[269]

While confidentiality assurances provide strong protections of privacy, they are subject to significant limitations. Confidentiality assurances are available for all research projects, and federal funding is not required. However, the policy of the Assistant Secretary is that certificates are issued "sparingly," that is, "only when the research is of a sensitive nature where the protection is judged necessary to achieve the research objectives."[270] Moreover, even where a certificate is issued, protection does not extend to voluntary disclosure by the researcher. Furthermore, the protection does not apply to disclosure if the subject or guardian consents either to demands for information for audit by the funding agency or to access to records by the federal Food and Drug Administration. Technically, the certificate appears to relieve researchers from the obligation to comply with legal requirements to report conditions such as child abuse or communicable diseases. However, if the researcher seeks a certificate to avoid reporting a communicable disease, the Assistant Secretary requires a special showing on how the research would be impaired by the reporting.[271] As with other federal provisions, the protection afforded by confidentiality assurances remains limited by loopholes and exceptions.

6. *State Privacy Legislation*

States have enacted health information privacy protection in highly diverse ways, including statutes modeled after the federal Privacy Act[272] and FOIA.[273] A few states have comprehensive medical information statutes. California, for example, prohibits providers from disclosing identifiable health information without the patient's written consent, unless the disclosure is required or authorized by

266 Assistant Secretary for Health, Interim Policy Statement (June 8, 1989).

267 *Id.*

268 *Id.*

269 *Id.*

270 *Id.*

271 *Id.*

272 *See, e.g.*, N.Y. PUB. OFF. LAW §§ 91-99 (McKinney 1988 & Supp. 1995).

273 *See, e.g.*, MISS. CODE ANN. §§ 25-61-1 et seq. (1991).

law.[274] The California statute authorizes the release of information necessary for payment for health services.[275]

State "practice acts" that license physicians, nurses, or other health care professionals and state statutes that regulate hospitals or other institutions frequently contain provisions limiting unauthorized disclosures of confidential patient information.[276] These statutes often contemplate or require maintenance of manual patient records, leaving the scope of protection afforded to automated records uncertain.[277] In addition, most states do little to regulate the informational practices of insurers; only 14 states have adopted model privacy legislation drafted by the National Association of Insurance Commissioners.[278]

(i) *The patient-provider privilege*—The patient-provider privilege, adopted in different forms in many states, plays a limited role in protecting privacy. It is typically a testimonial privilege, not a general obligation to maintain confidentiality. While the privilege may permit health care professionals to refuse to disclose information about patients in court, it usually does not prevent extra-judicial disclosure to employers or insurers. The privilege is often subject to important exceptions. For example, it does not apply where the patient puts his or her physical or mental condition at issue in a court case (involving, for example, personal injury or the insanity defense) or in physician licensure proceedings.

The patient-provider privilege applies only to disclosures made in the course of narrowly specified relationships. In many states, the privilege is limited to physicians and therapists and does not extend to the great majority of health care professionals.[279] Nor does the privilege apply to self help groups or other noncertified therapists. Indeed, the privilege usually extends only to communications between two people; although "family and group therapists may request that their patients keep sessions confidential, the patients themselves are not legally bound to do so."[280] Even when a privilege is recognized

---

274 CAL. CIV. CODE §§ 56-56.37 (West 1982 & Supp. 1995).

275 *Id.*

276 *See* Felis v. Greenberg, 273 N.Y.S.2d 288 (Sup. Ct. 1966) (liability imposed on doctors for violating a duty of confidentiality express or implied in state licensure or privilege statutes); Berry v. Moench, 331 P.2d 814, 817 (Utah 1958).

277 INSTITUTE OF MEDICINE, *supra* note 25, at 161-62; WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 4 at 12-13.

278 *See* GEORGE B. TRUBOW ET AL., PRIVACY LAW AND PRACTICE ¶ 801 (1991).

279 *See* BARRY R. FURROW ET AL., HEALTH LAW: CASES, MATERIALS AND PROBLEMS 221-22 (1987) (citing Barry B. Boyer, *Computerized Medical Records and the Right to Privacy: The Emerging Federal Response*, 25 BUFF. L. REV. 37, 75-79 (1975)).

280 Jan Hoffman, *Faith in Confidentiality of Therapy Is Shaken*, N.Y. TIMES, June 15, 1994, at A1, B5.

under state law, it may be treated as qualified, with courts weighing the need to have information against the social costs of not having it.

(ii) *Disease-specific statutes*—State law also contains a patchwork of privacy protection that is disease specific. Diseases that often receive special treatment include mental illness,[281] HIV infection or AIDS,[282] and sexually transmitted diseases.[283] Some states also specifically protect genomic information.[284] Sometimes these statutes confer powerful, near absolute, privacy protection. For example, a Massachusetts statute prohibits any disclosure of HIV test results without the person's consent.[285] Other statutes contain so many instances where personal information can be disclosed that the exceptions swallow the privacy rule. A Connecticut statute protecting the confidentiality of a person's HIV status allows disclosure to dozens of individuals, including health care professionals, laboratory technicians, and emergency workers.[286] In general, the problems with disease-specific legislation described above in relation to the federal alcohol and drug regulations apply equally to those adopted at the state level.[287]

C. Common-Law Protection of Health Informational Privacy

Most states recognize a common-law duty of confidentiality applying to certain health care professionals. Thus, if a patient divulges personal information to a health care professional believing that it is private, the professional may be liable for extra-judicial disclosure without the patient's consent or another valid justification.[288] This has been described as the breach of confidentiality tort,[289] although courts have relied on various theories of recovery,[290] including inva-

---

281 *See, e.g.*, ILL. REV. STAT. ch. 740 Para. 110/1 (1989).

282 *See* Harold Edgar & Hazel Sandomire, *Medical Privacy Issues in the Age of AIDS: Legislative Options*, 16 AM. J.L. & MED. 155 (1990) (examining state legislation dealing with HIV related problems in medical privacy laws).

283 *See* Gostin, *supra* note 150, at 463-65 (arguing immediate reform of the states' public health statutes to respond to modern notions of disease and privacy).

284 *See* Gostin, *supra* note 178, at 109 (suggesting that the federal government should close the gap between technological advances in genetic testing and the laws governing use of information gained through testing).

285 MASS. ANN. LAWS ch. 111 § 70f (Law. Co-op. 1985 & Supp. 1994).

286 CONN. GEN. STAT. § 19a-583 (1992).

287 *See supra* part III.B.3.

288 *See, e.g.*, Humphers v. First Interstate Bank, 696 P.2d 527 (Or. 1985) (en banc).

289 Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982).

290 *See id.* at 1437-48; TURKINGTON, *supra* note 212, at 318-20; WORKGROUP FOR ELECTRONIC DATA INTERCHANGE, *supra* note 30, app. 4 at 15-16.

sion of privacy,[291] implied term of contract,[292] and breach of fiduciary relationship.[293] Courts have upheld breach of confidentiality claims when the physician made an unauthorized disclosure of information obtained in the course of a therapeutic relationship with employers[294] or family members.[295]

These claims are weakened to the extent that courts recognize justifications other than consent. The primary justification[296] for nonconsensual disclosure is to protect a third party against a significant risk of harm, such as contracting a communicable or sexually transmitted infection[297] or physical injury.[298] Some courts, when faced with an immediate and significant risk to an identifiable person, impose a duty to protect which may include a duty to inform.[299] Other

---

291 The invasion of privacy theory effectuates the interest implicated in publicity cases, in which a person's reputation is at stake. The tort has significant doctrinal limitations in providing an adequate remedy for breach of confidentiality because it typically requires broad publication of the private matter, the public interest in knowing about public events or public figures may defeat the claim, and truth may be a defense. In fact, there may be four distinct branches of tort involved in an invasion of privacy theory: "intrusion upon seclusion," "appropriation of name or likeness," "publicity given to private life," and "publicity placing person in false light." RESTATEMENT (SECOND) OF TORTS § 652B-E (1977).

292 Courts sometimes incorporate a duty of confidentiality into an implied service contract between the physician and patient. The expectation of confidentiality in the physician-patient relationship may be inferred from the ethical codes of medicine, the law of the state (e.g., licensing requirements), or public policy favoring a strong therapeutic relationship, such as the maintenance of trust between doctor and patient. *See, e.g.*, Hammonds v. Aetna Casualty & Surety Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965) (implying as a condition of the contract that "the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission"); Doe v. Roe, 400 N.Y.S.2d 668, 674 (Sup. Ct. 1977).

293 Some courts see the therapeutic relationship as imposing on the physician a fiduciary duty to the patient. A disclosure of private information without appropriate justification is deemed a breach of the fiduciary obligation. *See* Ritter v. Rush-Presbyterian-St. Luke's Medical Ctr., 532 N.E.2d 327, 331 (Ill. 1988); Alexander v. Knight, 177 A.2d 142 (Pa. 1962).

294 *See* Horne v. Patton, 287 So. 2d 824, 830-31 (Ala. 1973); Alberts v. Devine, 479 N.E.2d 113, 118 (Mass. 1985), *cert. denied*, 474 U.S. 1013 (1985).

295 *See* Humphers v. First Interstate Bank, 696 P.2d 527, 530 (Or. 1985) (en banc); MacDonald v. Clinger, 446 N.Y.S.2d 801, 806 (1982).

296 Other justifications for disclosing confidential information include the patient's therapeutic interests, such as when a clinical record is provided to another health care professional responsible for the patient's care, and public health, such as when information is disclosed pursuant to a statutory reporting requirement. *See* Estate of Behringer v. Medical Ctr. at Princeton, 592 A.2d 1251, 1268-1269 (N.J. Super. 1991).

297 *See* Hofmann v. Blackmon, 241 So. 2d 752, 753 (Fla. Dist. Ct. App. 1970) (finding doctor liable to persons infected by his patient for negligent failure to diagnose a contagious disease); Wojcik v. Aluminum Co. of Am., 183 N.Y.S.2d 351, 357-58 (1959) (having diagnosed a contagious disease, doctor under duty to warn members of the patient's family).

298 *See MacDonald*, 446 N.Y.S.2d 801; Tarasoff v. Regents of University of California, 551 P.2d 334, 345 (Cal. 1976).

299 *See, e.g.*, Lipari v. Sears, Roebuck & Co., 497 F. Supp. 185, 189 (D. Neb. 1980); *see also* Alan A. Stone, *The Tarasoff Decision: Suing Psychotherapists to Safeguard Society*, 90 HARV.

courts have permitted disclosures to protect third parties without creating a legal obligation to disclose.[300]

While common law protection of confidentiality probably provides the most consistent safeguards, siguificant gaps exist in legal duties. Although most states recoguize a duty of confidence inherent in the physician-patient relationship, some jurisdictions do not.[301] Even in jurisdictions that uphold claims for breach of confidence, courts may limit the claims to physicians; it is at best uncertain whether a duty of confidentiality extends to other health care professionals, researchers, or health care institutions, although the risk of harm from disclosure is just as significant.[302] The breach of confidentiality tort usually requires a special kind of relationship, one in which the patient is able to demonstrate a clear expectation of privacy. When information is disclosed in the absence of this type of relationship or when the nature of the relationship itself is ambiguous (e.g., discussions with a doctor acting for an insurance company), a duty of confidence may not exist.[303] Physicians in many sectors of society may play dual roles and have divided loyalties (e.g., physicians practicing in prisons, in the military,[304] or in workplace settings such as employee assistance programs).[305] In these settings, courts may determine that

---

L. REV. 358 (1976); Toni P. Wise, Note, *Where the Public Peril Begins: A Survey of Psychotherapists to Determine the Effects of* Tarasoff, 31 STAN. L. REV. 165 (1978).

300 *See* Alberts v. Devine, 479 N.E.2d 113, 115 (Mass. 1985), *cert. denied*, 474 U.S. 1013 (1985).

301 *See* Mikel v. Abrams, 541 F. Supp. 591 (W.D. Mo. 1982), *aff'd*, 716 F.2d 907 (8th Cir. 1983); Collins v. Howard, 156 F. Supp. 322, 324 (S.D. Ga. 1957); Coralluzzo *ex rel.* Coralluzzo v. Fass, 450 So. 2d 858, 859 (Fla. 1984).

302 *See Collins*, 156 F. Supp. at 324; Quarles v. Sutherland, 389 S.W.2d 249 (Tenn. 1964); *but see* Estate of Behringer v. Medical Ctr. at Princeton, 592 A.2d 1251, 1271 (N.J. Super. 1991) (holding that hospital as well as the health care professional has a duty to protect confidentiality by establishing rigorous policies and procedures to prevent unauthorized disclosure of information).

303 *See* Hague v. Williams, 181 A.2d 345, 349 (N.J. 1962) (finding that both a public and private interest militates against an obligation of confidentiality with respect to disclosure of a child's condition to an insurer).

304 Martin Kasindorf, *FOCUS ON: Gays in Military; Threat of Dismissal Still Real*, N.Y. NEWSDAY, June 24, 1994, at A15 (Serviceman's divulgence of his suspicion that he may be gay to Marine Corps psychiatrist was disclosed to his supervisors, with the possibility of termination from the Marines.).

305 Employee assistance programs (EAPs) provide a particularly interesting illustration of the problematic protection of privacy afforded by the law. EAPs, available to approximately half of all U.S. employees, are presented as a free benefit for dealing with medical and mental health problems. To many employees, there is an expectation of confidentiality, particularly because personal disclosures are frequently made to physicians or counsellors. Yet, employers can lawfully obtain personal health data in diverse ways: when an employee files a workplace injury claim, EAP records are often turned over to claims adjusters; if the employee sues for wrongful dismissal, discrimination, or breach of contract, employers may be permitted to defend the claim using employee records; if the employee is suicidal, threatens violence, or has reported child abuse, the EAP may be permitted or required to notify government authorities; or if the supervisor suggests that the employee

there is no clear duty to maintain confidentiality if the role relationship cannot be characterized as one involving a physician and a patient.[306] Finally, a tort action usually will succeed only against the person who holds information in confidence.[307] Since the "holder" of the information can be unclear in a national or regional automated health information system, a duty in tort may have questionable utility.[308]

D. Theoretical Problems with the Current Legal Protection of Informational Privacy

The foregoing discussion suggests the existence of significant doctrinal limitations in the law relating to breach of confidentiality: legal protection is premised on the existence of a relationship between a physician and a patient, although most health information is not generated within this relationship; and the duty holder is the individual or institution that is in physical possession of the record, although no one actually "holds" electronic data. Legal protection that is centered on either of these premises has a distinct obsolescence in an information society.

The tort rule that enforces a person's right to confidentiality in the health care setting is grounded in the special relationship between the physician and the patient. The law of confidentiality is justified by the need to develop trust in the physician, so that patients will feel free to disclose the most intimate aspects of their lives. Confidentiality, therefore, is designed both to enhance the therapeutic process, by encouraging disclosures that assist in accurate diagnosis and effective treatment, and to strengthen the bonds of the physician-patient relationship as a general social good.[309]

The rule of confidentiality is widely respected in law and medicine, and rightfully so. Indeed, in the past, confidentiality has worked reasonably well in safeguarding privacy. Much, if not all, of the intimate knowledge of the patient was generated within the physician-patient relationship, which was often meaningful and endur-

---

contact the EAP, the supervisor may have the right to be informed of the visits (but not necessarily the contents). *See* Ellen E. Schultz, *If You Use Your Firm's Counselors, Remember Your Secrets Could Be Used Against You*, WALL ST. J., May 26, 1994, at C1; *see also* KURT H. DECKER, PRIVACY IN THE WORKPLACE: RIGHTS, PROCEDURES, AND POLICIES (1994); Ellen E. Schultz, *Medical Data Gathered by Firms Can Prove Less Than Confidential*, WALL ST. J., May 18, 1994, at A1 (documenting numerous instances of disclosures by EAP professionals to employers and insurers).

306 *See* Bratt v. International Bus. Mach. Corp., 785 F.2d 352, 357-58 (1st Cir. 1986).

307 *See* Humphers v. First Interstate Bank, 696 P.2d 527, 530 (Or. 1985) ("[O]nly one who holds the information in confidence can be charged with a breach of confidence.").

308 *See infra* notes 309-12 and accompanying text.

309 *See generally* Lawrence O. Gostin et al., *The Case Against Compulsory Casefinding in Controlling AIDS: Testing, Screening and Reporting*, 12 AM. J.L. & MED. 1, 45-47 (1987).

ing.[310] The patient's health record contained information primarily obtained during sessions between the physician and patient, so that the entire record was regarded as confidential. The record keepers, moreover, were the physicians themselves who took primary responsibility for the security of medical records.

The rule of confidentiality does not work nearly as well in a modern information society. Health data today, in an era of electronic information gathering, is based only in small part on the physician-patient relationship. Many therapeutic encounters in a managed care context are not with a primary care physician. Patients may see many different physicians, nonphysician specialists, nurse practitioners and other ancillary health care professionals within and outside of the health care plan. The information obtained in these encounters has uncertain protection under traditional rules of confidentiality.[311] Focusing legal protection on a single therapeutic relationship within this information environment is an anachronistic vestige of an earlier and simpler time in medicine. The health record, moreover, contains a substantial amount of information gathered from numerous primary and secondary sources: laboratories, pharmacies, schools, public health officials, researchers, insurers, and other individuals and institutions.[312] The health records of patients are kept not only in the office of a private physician or in a health plan, but also may be kept by government agencies, regional health database organizations, or information brokers. Databases maintained in each of these settings will be collected and transmitted electronically, reconfigured, and linked.[313]

Rules enforcing informational privacy in health care place a duty on the entity that possesses the information.[314] Thus, the keeper of the record—whether it is in a private physician's office, a hospital, or an HMO—holds the primary duty to maintain the confidentiality of the data. The development of electronic health care networks permitting standardized patient-based information to flow nationwide, and perhaps worldwide, means that the current privacy protection system, which focuses on requiring the institution to protect its records, needs to be reconsidered. Our past thinking assumed a paper or automated record created and protected by the provider. We must now envision a patient-based record that anyone in the system can call up on a

---

310 Admittedly, the romanticized view of the meaningful quality of the therapeutic relationship has been unraveled by a number of thoughtful scholars. Among the most telling critiques of the quality of that relationship is found in the work of JAY KATZ, THE SILENT WORLD OF THE DOCTOR AND PATIENT (1984).

311 *See supra* notes 283-90 and accompanying text.

312 *See supra* notes 60-77 and accompanying text.

313 *See supra* notes 61-77 and accompanying text.

314 *See supra* notes 249-60 and accompanying text.

screen. Because location has less meaning in an electronic world, protecting privacy requires attaching protection to the health record itself, rather than to the institution that generates it.

IV

UNIFORM NATIONAL STANDARDS FOR THE ACQUISITION AND DISCLOSURE OF HEALTH INFORMATION

The previous Parts of this Article marshalled the arguments justifying the construction of a health information system and discussed some significant privacy concerns. This Part seeks to demonstrate that, while privacy is an important human value, it does not transcend other values served by comprehensive health information. Next, this Part explains why enacting uniform national standards is most likely to be effective in ensuring fair informational practices in the health care system.[315] Finally, this Part sets out the primary conceptual elements of a proposed national policy.

A. Ethical Justifications for a Health Information Infrastructure

While it would be comforting to assume that society could achieve both the benefits of health information and reasonable levels of privacy, it is unlikely that this will occur. There are simply too many opportunities for use of health data in ways that are inconsistent with the desires of patients for privacy. Given a hard choice, privacy advocates might argue for the abandonment of, or a reduction in, the plans for a comprehensive health information infrastructure. After all, the primary justifications for collection of health data—e.g., efficient administration and cost reduction—appear to be purely instrumental. However, a careful examination of the ethical justifications for privacy show that privacy's moral value also is in the main derivative and based on utilitarian concerns.

The literature on privacy abounds with accounts of the moral justifications for rules of privacy. One standard account holds that the primary justification for respecting privacy resides in the principle of respect for autonomy. To respect the privacy of others is to respect

---

315 The Working Group on Privacy of the Information Policy Committee of the (Interagency) Information Infrastructure Task Force published an update of the Code of Fair Information Practices originally developed in the early 1970s. The "Draft Principles for Providing and Using Personal Information" include: (1) a collection principle so that individuals are provided information on how data will be used and protected; (2) an acquisition and use principle, so that users of personal information must assess the impact on privacy of data collection; (3) an education principle, so that the public will be educated about the national information infrastructure; and (4) a fairness principle, so that individuals can obtain, review, and correct their own information. Office of Management and Budget, Draft Principles for Providing and Using Personal Information, 59 Fed. Reg. 27,206 (1994).

their autonomous wishes not to be accessed in some respect—not to be observed or have information about themselves made available to others.

Respecting privacy is also an important means of fostering and developing a sense of self and of personhood. It is difficult to imagine how, in the absence of some level of privacy, individuals can formulate autonomous preferences or, more basically, develop the capacity to be self-governing. On this account, certain conditions of privacy are viewed as necessary for the development or at least the fostering of personhood.

Finally, privacy enhances the development and maintenance of intimate human relationships—relations of trust, friendship, and love. It is arguably one of the defining characteristics of intimate relationships that they involve the sharing—freely given—of private information, spaces, and acts. An expectation of privacy allows individuals to confide freely in their physicians and other confidants about the most sensitive of issues.

The ethical justifications for informational privacy also point to a variety of economic harms that may result from unwanted disclosures of personal health information, such as loss of employment, insurance, or housing, as well as social or psychological harms. Enforcing rules of privacy, then, can avoid many harms for individuals that flow from the unauthorized disclosure of confidences.

Despite the well-founded claims for respecting the privacy of individuals, it is important to emphasize that many careful observers do not see privacy as an intrinsic value. To a large extent, privacy is derivative of other, more fundamental, ethical principles such as autonomy and respect for persons. Furthermore, to the extent that ethical justifications rely on the harms resulting from the nonobservance of its rules, privacy is of instrumental value. Privacy is important primarily because of its utilitarian features—e.g., it promotes more effective communication between physician and patient, enhances autonomy, and prevents economic harm, embarrassment, and discrimination.

It would, therefore, be a mischaracterization of the ethical arguments to assume the preeminence of privacy because of its normative or intrinsic values. Equally compelling ethical claims can be made to support a more efficient health information system. Like the justifications for privacy, these ethical arguments are principally derivative and instrumental in value. Although justifications for privacy are based primarily on goods for the individual, justifications for more efficient health information are based primarily on societal or collective goods.

To the extent that more efficient use of health information would promote access to health care, more equitable distribution of services

to vulnerable populations, higher quality, better research, and more effective public health interventions, substantial ethical values militate in favor of its rapid development. The very purpose of government is to attain through collective action human goods that individuals acting alone could not realistically achieve.[316] Chief among those human goods is the assurance of the conditions under which people can be healthy.[317] While the government cannot assure health, it can, within the reasonable limits of its resources, organize its activities in ways that best prevent illness and disability, and promote health among its population.

Health is basic to all human endeavors and, therefore, may be regarded as a foundational justification for government action.[318] Health is a necessary condition for the pursuit of livelihood, the exercise of fundamental rights and privileges, and the achievement of personal satisfaction. Certainly, health information is not sufficient to achieve all of these goals, but it is arguably a necessary condition for more cost-effective health services.

It is not my intention here to argue which is the most important human good—health or personal privacy. Moreover, a rigorous moral theory does not exist that demonstrates the primacy of one value over the other. It is possible, however, to propose a social contract that reasonably balances both human goods, while declaring neither the winner.

Individuals already forego significant levels of privacy in order to obtain the social goods that benefit society collectively. Many of the collective goals in society, ranging from law enforcement and public safety to tax collection and national security, are achieved partly by substantial collection of personal information. Not every individual agrees with this social contract, but all individuals benefit and, as citizens of the wider community with the right of franchise, we accept the need for diminution in individual autonomy and privacy in exchange for substantial collective benefits. A complex modern society cannot elevate each person's interest in privacy above other important societal interests.

As the United States intensely considers the values and effectiveness of its health care system, it must acknowledge that one of the burdens of achieving cost effective and accessible care is a loss of pri-

316 *See generally* MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY 64-91 (1982).

317 "Public health is what we, as a society, do collectively to assure the conditions in which people can be healthy." INSTITUTE OF MEDICINE, *supra* note 147, at 19, 36-38.

318 *See* NORMAN DANIELS, JUST HEALTH CARE (1985); Dan W. Brock & Norman Daniels, *Ethical Foundations of the Clinton Administration's Proposed Health Care System*, 271 JAMA 1189 (1994); Charles J. Dougherty, *Ethical Values at Stake in Health Care Reform*, 268 JAMA 2409 (1992).

vacy. In exchange for this diminution in individual rights, the government is obliged to create reasonably strong assurances of fair informational practices, without losing the benefits of a health information system.

B. Justifications for a Preemptive Federal Statute: Thoughtful Federalism

Continued reliance upon current legal safeguards is incompatible with the policy objectives of an integrated health information system for a number of reasons. A state-by-state approach to regulation of medical information does not reflect the realities of modern health care finance and delivery. The flow of medical information is rarely restricted to the state in which it is generated. Such information is routinely transmitted to other states, subject to differing legal requirements, for a wide variety of purposes ranging from medical consultation and research collaboration to governmental monitoring for quality.

Further, the physical location of health information is no longer relevant. Databases containing huge quantities of personal information provide immediate access to a variety of eligible users in remote locations. Thus, laws that attempt to regulate information physically located in a particular state are ill suited to the need for efficient collection of information and the enforcement of reasonable levels of privacy in a postelectronic era.

The prospect for resolving these problems through the enactment of model or uniform laws in every state is exceedingly small. The National Conference of Commissioners on Uniform State Laws adopted the Uniform Health Care Information Act in 1985,[319] but only two states, Montana and Washington, have enacted it.[320]

The absence of a uniform health information policy imposes hardships on virtually all concerned. Health care institutions, insurance companies, and self-insured employers who transmit health data through interstate commerce often do so without clear guidance regarding which state's laws govern or which state's courts have proper jurisdiction to resolve disputes that may arise. Without the ability to know and to rely on uniform regulation of information, patients lack the basis for meaningful consent to disclosure. Lack of uniformity adversely affects the integrity of health data, and the quality of care itself, by undermining efforts to automate health records. These detriments of state-by-state regulation of information would only be magnified in a national health care system in which patients are entitled to cover-

319 UNIFORM HEALTH CARE INFORMATION ACT (1985).

320 MONT. CODE ANN. § 50-16-501 (1993); WASH. REV. CODE ANN. § 70.02.005 (West 1992).

age anywhere they live in the country and information for monitoring quality and cost effectiveness is collected regionally, if not nationally. Consequently, many persuasive reasons exist to adopt a uniform federal health information policy that transcends state borders.

Critics of preemption base their arguments on two points. First, a preemption strategy does not permit states to create stronger rules of privacy: if a state legislature were to give greater credence to the value of privacy, it could not act in the face of a preemptive federal statute. While many would not wish to prevent states from giving more rights to privacy than are provided at the federal level, allowing such state action would defeat the chief goal of a preemption strategy. By permitting greater protection of privacy, a state would impede the free flow of information across state lines. This is precisely what a preemption strategy would seek to prevent.

The second point is more general in nature. Critics argue that preemption virtually eliminates experimentation by the states. Encouraging states to find model solutions to complex problems—a particularly attractive feature of our federalism—is defeated by preemption. While this aspect of federalism can be important, there are sound reasons for reducing, if not eliminating, the variability of state rules protecting privacy. Both people and personal data travel freely across state lines, sometimes for a single course of treatment. For example, a patient may be treated in an emergency room in one state, return to his or her home state for continuing treatment, and fly to yet another state for specialist care. Data about that individual would circulate still more widely for medical consultations, quality assurance, and reimbursement. Patients, health care providers, employers, and insurers should not have to speculate as to which state's privacy rules apply and what level of legal protection the data are afforded. Permitting state experimentation would impede the free flow of information and leave the level of protection uncertain. This is not the result that thoughtful federalism would welcome.

C. Structuring Legal Regulation to Use Information as a Resource for the Health of the Community, Consistent with Obligations to Individuals

In an ideal world, the nation would develop a health information system and promise complete privacy to its citizens. Realistically, though, a promise of complete privacy must be hollow; it cannot be faithfully made or kept. What our government can do is create fair, comprehensive rules, applicable throughout the United States, to ensure that information is acquired, used, and disseminated according to clearly understood criteria and procedures, under mandated secur-

ity arrangements.[321] This Part suggests ways to structure the law to allow information to be used as a resource for the health of the community, consistent with the obligation to utilize personal information fairly.

A foundational question for the development of a federal preemptive statute is where its rules should apply. A new conceptualization of health information privacy would move beyond the traditional approach of protecting the confidentiality of the therapeutic relationship and placing duties on the physical keeper of the record.[322] Rather, the rules need to follow the health information itself. Any data acquired, collected, used, or disseminated within the health care system should be protected. The health care system should be construed broadly to include diagnosis, treatment, payment, and oversight related to the provision of any health services. Thus, all the information in the patient's longitudinal health record should be protected, irrespective of its origin (within the therapeutic relationship or elsewhere), use (for treatment, quality assessment, or research), medium (oral, recorded, paper, microfilm, or electronic), location (in storage, transit, or archive), dissemination (whether sent to payers, public health departments, or employers), and user (government, health provider, or private organization).

The rules for limiting the flow of data ought to apply equally to all information, whether it is within the government mandated health care system or outside it. Some reform proposals provide protection only for data within the statutorily created health system; health data generated or used outside of the system (e.g., for health services purchased privately that are not covered by the guaranteed benefits package) would not be protected.[323] These proposals would be both unjust and impractical. A patient's expectation of privacy remains the same whether the services are government mandated or privately purchased. Although the government may have a stronger claim to regulate information practices within the system it establishes, the *raison d'être* for fair information practices (providing minimum levels of privacy and control of personal information) is the same within and outside of the official health care system. Also, as a practical matter, it would be difficult to track the flow of information to determine whether it deserves "in system" protection. Electronic data flow freely across systems, rendering fine distinctions unworkable.

---

321 In order to ensure that the privacy of health care data is taken seriously, it will be necessary to establish effective mechanisms for enforcement. This includes a private right of action by aggrieved parties and significant penalties for persons or institutions that breach legal requirements.

322 *See supra* notes 287-307 and accompanying text.

323 *See, e.g.*, Health Security Act, *supra* note 88, § 5120 (Privacy standards are applicable only to health information that is regnlated by the National Health Board.).

A national health information policy should establish uniform and comprehensive protection to replace the current patchwork of federal and state legislation. A thoughtful structure for balancing collective interests in health and individual interests in privacy would consider a number of separate issues. First, not all data are the same. Depending on the method of collection, storage, and use, data may warrant different levels of privacy protection. Second, depending on the level of privacy to be afforded, a substantive and procedural review of the purported justification for the collection, use, and reuse of the data is necessary. Third, if the individual has some right to control the use of his or her own record, it is necessary to determine the degree of autonomy that ought to be afforded. Fourth, if data can only be used for the legitimate and limited purposes for which they were acquired, it is necessary to determine if there are circumstances when they could be used without the patient's consent. Finally, we should select or create an entity to oversee the national information infrastructure, to ensure that comprehensive and accurate health data are available in the public interest with a minimum diminution of individual privacy.

1. *The Level of Privacy Protection Warranted: The Nature of the Data—Personally Identifiable, Linkable, or Anonymous*

Most legislative proposals protect only individually identifiable health information.[324] Yet, health information takes many forms, each raising distinct concerns about privacy. The most serious privacy concerns involve information that is identifiable so that others can directly associate a record with a particular person. The inclusion of any uniquely identifiable characteristic, such as a name, social security number, finger print, or genetic link, classifies data as identifiable. Information on health care records used for clinical treatment is ordinarily unique and can be linked to a particular person. In addition, many researchers use identifiers for longitudinal follow-up of the subject.

Information that is anonymous and nonlinkable poses the fewest privacy concerns. Data that have all identifiers stripped, with no means to associate the information with a specific person, are anonymous. Epidemiological research and surveillance activities such as anonymous, unlinked serologic surveys are often structured so that the data are anonymous. For example, many HIV seroprevalence studies conducted from blood specimens left over from some other lawful activity have not used identifiers.

---

324 *See id.* § 5120(a) ("individually identifiable health information"); Fair Health Information Practices Act of 1994, H.R. 4077, 103d Cong., 2d Sess. § 3(a)(3)(B)(ii) (data that identifies the individual or can be used to readily identify the individual).

Information that is ostensibly anonymous but can be linked to a person presents an intermediate level of privacy concern. Some epidemiologic research and databases are structured so that anonymous information can only be linked to a specific person with the use of a highly confidential code. Data often remain linked to permit future disclosure of test results or other data deemed vital to the health or safety of the patient or others—for example, to inform the patient or others of an infectious disease or genetic trait that would be helpful in behavioral, therapeutic, or reproductive decisions. The ability to link data, however, can cause considerable controversy. New York State, for example, considered unlinking HIV serologic data among pregnant women because of the research finding that treatment of the woman and newborn with antiviral medication significantly reduces the risk of vertical transmission of HIV.[325] Yet, linking the data poses a potentially momentous invasion of privacy. Women who might not wish to know their HIV status would have knowledge of a terminal illness imposed on them without their consent[326] and might be subject to discrimination.[327]

In determining the level of privacy protection warranted, a rigorous evaluation of the nature of the data held is essential. Not all data raise the same level of privacy concerns nor warrant the same level of legal protection. In general, the level of privacy protection warranted increases as the data become more personally recognizable, from anonymous, to linkable, to identifiable.

While patients have a weaker claim to control the use of nonidentifiable data because they are less likely to suffer personal harm by the disclosure, it would be wrong to assume that no valid interests exist in anonymous information. Some records do not readily identify individuals but can identify members of discrete populations. Although the data do not identify any individual, persons in the group may feel embarrassed or the data may reflect badly on the self-identity or integrity of the group. Collection of highly sensitive data may identify a small group such as a high school in a rural community, a racial or ethnic group such as an American Indian tribe, or a vulnerable population such as a poor African-American or Hispanic neighborhood.

---

325 Edward M. Connor et al., *Reduction of Maternal-Infant Transmission of Human Immunodeficiency Virus Type 1 with Zidovudine Treatment*, 331 NEW ENG. J. MED. 1173, 1178 (1994) (Administration of zidovudine (AZT) to the mother during pregnancy and during labor and delivery and giving it to the infant for the first six weeks of life reduced the risk of maternal-infant transmission of HIV approximately two thirds.).

326 Compulsory testing and treatment of the mother may or may not be considered a moral wrong when balanced against the strong benefit to the infant. *See* Ronald Bayer, *Ethical Challenges Posed by Zidovudine Treatment to Reduce Vertical Transmission of HIV*, 331 NEW ENG. J. MED. 1223 (1994).

327 *See* Martha F. Rogers & Harold W. Jaffe, *Reducing the Risk of Maternal-Infant Transmission of HIV: A Door is Opened*, 331 NEW ENG. J. MED. 1222 (1994).

For example, data showing a disproportionately high rate of HIV infection, mental illness, alcoholism, or sexually transmitted disease in discrete populations can serve important public health purposes, but can also be offensive and sometimes misleading. Ideally, patients should be informed if data are to be released to public health officials, risk managers, or researchers in nonidentifiable form, even if a requirement of informed consent for use of the data would be overly restrictive.[328] The individual's claim to control the flow of linkable data depends on the degree of protection afforded to prevent unauthorized identification of the record; the greater the privacy and security afforded to the record, the less the patient's claim to control its release.

2. *Substantive and Procedural Review for the Acquisition or Use of Data*

As will be shown,[329] many see the collection of health data as an inherent good. Even if the social good to be achieved is not immediately apparent, it is always possible that some future benefit could accrue. A technological breakthrough may mean that some clinical value could be achieved later by collecting data today. But despite optimism in the power of future technology, the diminution in privacy attributable to the collection of health data demands that the acquisition of information serve some substantial interest. The burden rests on the collector of information, not merely to assert a substantial public interest, but to demonstrate that it would be achieved. Information should only be collected under the following conditions: (1) the need for the information is substantial; (2) the collection of the data would actually achieve the objective; (3) the purpose could not be achieved without the collection of identifiable information; and (4) the data would be held only for a period necessary to meet the valid objectives.

The collection of large amounts of health information requires not only a substantive justification, it also warrants procedural review. For example, the development of a large database, such as a tissue repository, can have a profound effect on the privacy of individuals and populations. Decisions to create health databases, whether by government or in the private sector, ought to require procedural review. Some mechanism for independent review by a dispassionate expert body at a regional or national level would provide a forum for careful examination of the justification for the collection of data, the

---

328 *See* COUNCIL OF INT'L ORG. OF MEDICAL SCIENCES, INTERNATIONAL ETHICAL GUIDELINES FOR EPIDEMIOLOGIC RESEARCH (1992).

329 *See supra* notes 95-97 and accompanying text.

existence of thoughtful consent procedures, and the maintenance of adequate privacy and security.

3. *The Autonomy of the Individual to Control Personal Data: Informed Consent*

If a central ethical value behind privacy is respect for personal autonomy,[330] then individuals about whom data are collected must be afforded the right to know about and to approve the uses of those data. While legal and ethical discourse on informed consent has traditionally focused on the patient's assent to medical treatment, justifications for applying the doctrine to the release of information are equally valid. In each case the claim of the patient is to maintain control over events that deeply affect his or her life. Unwanted medical treatment is an invasion of the physical integrity of patients. Yet, the economic and personal consequences of unwanted disclosures of personal information can be just as real.

As in treatment decisions, consent for the collection, use, and reuse of information may be more illusory than real. The collectors of information may not seek consent, they may provide insufficient information to elicit a rational choice, and the consent form may be overly technical and difficult for a lay person to follow. Traditional doctrine on informed consent requires that a competent person have adequate information to make a genuinely informed choice.[331] However, few objective standards have been developed outside of the treatment context to measure the adequacy of consent.

To render consent meaningful, the consent process must incorporate clear content areas.[332] First, it is necessary to specify how privacy and security will be maintained. A simple assertion that privacy will be respected is insufficient if the person is unaware of the steps to be taken to protect sensitive data. Second, a statement indicating that the person is the owner of the data and can control the use of the data is important. Specific instructions on means of access, review, and correction of records would provide a practical means of exercising control over data. Third, a statement of the length of time that the information will be stored and the circumstances when it would be

---

330 *See* discussion *supra* part IV.A.

331 *See generally* PAUL S. APPELBAUM ET AL., INFORMED CONSENT: LEGAL THEORY AND CLINICAL PRACTICE 14 (1987) (Physicians must inform patients of the nature, purpose, risks, and benefits of any treatment they propose to perform); RUTH R. FADEN & THOMAS L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT (1986) (arguing that the ethical principle of autonomy justifies the doctrine of informed consent); Marjorie M. Shultz, *From Informed Consent to Patient Choice: A New Protected Interest*, 95 YALE L.J. 219 (1985) (recommending the creation of a legally protected right of patient autonomy).

332 The author appreciates the work in deriving these standards of Professor Robert Weir of the National Human Genome Project and Joan Porter of the Office of Protection from Research Risks of the National Institutes of Health.

expunged provides assurance that information will not be kept when it no longer serves an important public purpose. Fourth, a clear statement of the degree to which third parties—for example, relatives, regulators, researchers, and public health officials—will have access to the data is essential to understanding the level of privacy afforded. Individuals need to know if disclosure to third parties will require additional consent. Fifth, a clear statement about future secondary uses of the information would provide a better understanding of all possible uses to which the data will be put. Individuals ought to know if no secondary use will be made of the data, whether they will be given the option of not allowing the further disclosure, and whether they will be contacted in the future for additional consent.

A conceptual dilemma exists about whether to require consent for all secondary disclosures. Health care professionals traditionally make numerous disclosures that are considered "routine" and consistent with the purposes for which the data are held. Standard disclosures are made for treatment, payment, or oversight; to inform close family members; to protect the health of contacts of the patient or the public health; in emergency circumstances; when required by law such as with subpoenas and warrants or mandatory reporting; research; and law enforcement.[333]

The theory behind many of these routine disclosures has never been adequately explained. Some regard the disclosures as justified by express or implied consent, particularly when the release of information is intended for the patient's medical or financial benefit. Thus, the patient consents, or is presumed to consent, to the disclosure of information to other health care professionals to provide appropriate treatment, to insurers to assure payment, or to researchers or regulators to maintain effective oversight or evaluation of services. More careful thought about these disclosures reveals that they are not always justified by the autonomous and voluntary consent of the patient. Consent may be presumed in many cases by the person's desire to have the most effective treatment provided and paid for. However, not every patient will trust the receiver of the information to preserve his or her privacy; some insurers, for example, might use the data to deny insurance coverage, and some providers may disclose the information to family or friends. Even if the patient explicitly consents, it cannot be regarded as voluntary, for the consequence of refusal may be the denial of services or reimbursement. Disclosure of personal information without the meaningful consent of the patient, therefore, requires a convincing justification beyond consent—for example, for

333 These traditional uses of health data track the categories for disclosure of health information without patient authorization by health use trustees in the Fair Health Information Practices Act of 1994, H.R. 4077, 103d Cong., 2d Sess. §§ 122-30 (1994).

reasons relating to the efficient delivery and financing of health services.

Informed consent, in its best sense, is founded on an interactive, meaningful dialogue between a health care professional and patient. Creative and responsive informed consent procedures can readily be built into automated systems to supplement this personal dialogue. These include automatic reminders of the need to obtain consent before disclosure and of the need to renew an informed consent statement after the lapse of an agreed upon time.

4. *The Autonomy of the Individual to Control Personal Data: Right to Review and Correct Personal Data*

A central tenet of fair information practices is that individuals have the right to review data about themselves and to correct or amend inaccurate or incomplete records.[334] This right respects a person's autonomy, while assuring the integrity of data. Individuals cannot meaningfully control the use of personal data unless they are fully aware of their contents and can assess the integrity of the information. Patients' confidence in the storage, use, or dissemination of personal data often depends on the nature of the information in the file (how sensitive it is to the particular patient), and whether it is reliable. Patients are most likely to have confidence in personal data systems if they know the contents, have the opportunity to correct inaccuracies, and can control their use.

Patients can also help determine if the record is accurate, trustworthy, and complete. Health data can only achieve essential societal purposes if they are correct and reasonably comprehensive. While patients do not always have a detached and factual perspective on their own records, they can identify inaccuracies or omissions. One method, therefore, of ensuring the reliability of health records is to provide a full and fair procedure to challenge the accuracy of records and to make corrections.

5. *Use of Data for Intended Purposes: Health Information Trustees*

Entities that possess information have obligations that go beyond their own needs and interests. In some sense, they hold the information on behalf of the individual and, more generally, for the benefit of all patients in the health system. A confidence is reposed in a profes-

334 At present, patients have a statutory right of access to their own health records in approximately two-thirds of the states. JOHN CONTRUBIS, PATIENT ACCESS TO MEDICAL RECORDS: A STATUTORY SURVEY OF THE UNITED STATES 1 (1992). Some limitations may have to be placed on access of patients to their records if, for example, the data identify another individual and access would violate that person's privacy or would be harmful, or disclosure would pose a risk to the safety of others.

sional who possesses personal information for the benefit of others. It is for that reason that under some conceptions, the holders of data are referred to as "health information trustees."[335] Health information trustees have an obligation to use health information only for limited purposes (a limited use rule); to disclose information only for purposes strictly compatible with the purpose for which the data were obtained (a limited disclosure rule); to curtail disclosure to the minimum necessary to accomplish the purpose (a minimum disclosure rule); and to maintain an accounting for any disclosure (an accounting for disclosure rule).[336]

To some, the collection of ever-greater quantities of health data is important, irrespective of any coherent justification. Data, however, are not inherently good and need careful justification for their acquisition or disclosure. If society asks individuals to forego some level of privacy in exchange for a collective benefit, then the entity acquiring the data has a burden to demonstrate that a legitimate health-related purpose is furthered by the collection of the data. These limited purposes could be specifically authorized in legislation, and would include patient care, financing, regulatory oversight, public health, and research. If data were to be used for another valid purpose, it would require the person's informed consent or another substantial justification. Finally, data would be disposed of when no longer necessary to carry out the purposes for which they were collected.[337]

6. *Security of Health Information Systems*

The National Research Council observed that "[t]he nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security."[338] As automated systems increasingly contain standardized health information capable of being transmitted over electronic networks, "society becomes more vulnerable to poor systems design, accidents that disable systems, and attacks on computer systems."[339] While maintaining adequate security entails financial cost, the economic and privacy implications of leaving sensitive data inadequately secured would be considerable. Opportunities for using electronic networks may be lost if there is serious public mistrust of their safety.

---

335 *See* Fair Health Information Practices Act of 1994, H.R. 4077, 103d Cong., 2d Sess. § 101 (1994).

336 *Id.* § 121 (rules limiting trustees' use of information).

337 *See* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (Paris 1981).

338 SYSTEM SECURITY STUDY COMM., NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 2 (1991).

339 *Id.*

Although making a computer system one-hundred percent secure is not feasible, careful planning and use of technology can provide a great deal of protection of records.[340] Technological advances in electronic systems are proceeding at an accelerated pace. Data protection policies, if they are to be effective in this rapidly changing environment, cannot be tied to specific systems and system capabilities. Rather, government must establish security protection guidelines that define system goals but do not specify how these goals will be reached. The current voluntary process has not resulted in the development of a comprehensive set of standards, procedures, and practices needed to ensure the security of automated systems. The promulgation of national security standards and guidance would include the following elements: quality control, access control on code as well as data, user identification and authentication, protection of executable code, security logging, a security administrator, data encryption, operational support tools to assist in verifying the security state of the system, independent audits of the system, and hazard analysis.[341] Levels of access can also be established that recoguize the varying degrees of security required for differing kinds of information.[342]

---

340 *See* Colin J. Bennett, *Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s*, 16 SCI. TECH. & HUM. VALUES 51 (1991) (recommending a holistic approach to regulation that encompasses the relationship between organizational practices and information technology).

341 The creation of audit trails for monitoring all instances of access to and disclosure of automated health records on individuals involves computers producing logs of all instances when files have been accessed. The logs can be consulted by supervisors and security officers when complaints are received from individuals or when a suspicious pattern of access occurs. Thus, patterns of staff browsing in patients' records might be identified and questioned by data protection officers. *See generally* BRUCE, *supra* note 45, at 29-69 (suggesting procedural methods for health care providers to protect patient privacy); COMMISSION D'ACCES A L'INFORMATION, MINIMUM REQUIREMENTS FOR THE SECURITY OF COMPUTERIZED RECORDS OF HEALTH AND SOCIAL SERVICES NETWORK CLIENTS (April 1992); OTA DEFENDING SECRETS, *supra* note 58, at 131-48 (examining federal policies directed at protecting information in electronic communication systems); OTA FEDERAL GOVERNMENT TECHNOLOGY, *supra* note 6, at 99-125 (examining the federal use of electronic data bases and public policy concerning privacy); ROTHFEDER, *supra* note 170, at 124-52 (arguing that existing privacy protection laws are inadequate and advocating the establishment of a federal Data Protection Board; R. ROSENBERG, PRIVACY IN THE COMPUTER AGE (Computer Professionals for Social Responsibility, No. CL-100-3, 1989) (suggesting ways that individual and society can assure greater privacy).

342 *See* SYSTEM SECURITY STUDY COMMITTEE, *supra* note 337, at 80-88 (discussing different models that allow different levels of access); OTA PROTECTING PRIVACY, *supra* note 6, at 89-99 (discussing safeguards, e.g., cryptography, which can be used to ensure the privacy of medical records).

7. *Oversight of the Health Information System: Data Protection and Security Panel*

Establishing a National Data Protection and Security Panel would fill a major gap in America's privacy and security framework.[343] Such an entity would have several responsibilities essential for the development and implementation of effective privacy and security in the health care system. The panel would: (1) set privacy and security standards through interpretive rules, guidelines, or both that must be followed by participants in the health care system; (2) monitor and evaluate the implementation of standards set by statute, regulations, or guidelines; (3) sponsor or conduct research, studies, and investigations; (4) supplement other mechanisms in the health care system through which citizens question the propriety of information collected and used by various participants in the system; (5) advise the President, the Congress, government agencies, states, and other participants in the health care system; (6) support the development of fair and comprehensible consent processes governing the disclosure and re-disclosure of information to authorized persons, for authorized purposes, at authorized times; (7) fund pilot projects demonstrating the technology required for implementing security standards and sharing information in the health care setting; and (8) work with the health provider community to foster development of security practices responsive to their goals of providing effective health care.

CONCLUSION

A national health information policy that encourages the collection of vast amounts of electronic data while creating uniform rules for handling these data may be the best way of reconciling equally compelling public and private claims. Yet it remains far from perfect. To be sure, such a policy defeats legitimate privacy claims: it permits innumerable access by authorized professionals and organizations for treatment, reimbursement, regulation, research, and public health and fails to tightly circumscribe the scope of permissible disclosures or redisclosures for "compatible" or "routine" purposes. The potential for collection, matching, and reconfiguration of immense quantities of electronic data is real.

These human burdens in loss of privacy are not trivial. Yet, the need to measure the diminution in privacy against collective expecta-

---

343 The creation of a data protection entity has been recommended by members of Congress and by privacy experts. *See* Data Protection Act of 1991, H.R. 685, 102d Cong., 1st Sess. (1991) (Bill introduced by Rep. Wise would create a national board to recommend privacy protections for information); Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 GOV'T INFO. Q. 79 (1991) (arguing that a national board is necessary to provide a reasonable level of protection of information).

tions of considerable benefit under a national health care system is inescapable. As a general proposition, the government's claim of compelling advantage through collection of these data has been asserted with thought and rigor. This provides a general justification for development of the kind of ambitious health information system currently contemplated. But those who watch the government will insist on more. They will require that the laudable health goals asserted are actually achieved; that the social goods from collection of data are not assumed but are carefully justified before each disclosure; that less intrusive nonidentifiable data are used whenever they could achieve the asserted health objective; and that where privacy interests must be implicated, all holders of data comply with rigorous uniform standards established through federal legislation.